



Department of Computer Science and Engineering

CSE 3482 Introduction to Computer Security

Instructor: N. Vljic

Midterm Examination

Assignment Project Exam Help

Instructions:

- Examination time: 75 min.
- Print your name and CSE student number in the space provided below.
- This examination is closed book and closed notes.
- There are 6 questions. The points for each question are given in square brackets, next to the question title. The overall maximum score is 100.
- Answer each question in the space provided. If you need to continue an answer onto the last page, clearly indicate that and label the continuation with the question number.

<https://powcoder.com>

Add WeChat powcoder

FIRST NAME: _____

LAST NAME: _____

STUDENT #: _____

Question	Points
1	/ 20
2	/ 12
3	/ 10
4	/ 10
5	/ 34
6	/ 14
Total	/ 100

1. Multiple Choice

[16 points]

Circle the correct answer(s) to the following questions / statements. For each statement, you will obtain 0 marks if the number of circled answers is more/less than appropriate.

(1.1) Making sure that the data is accessible when and where it is needed is related to which of the following?

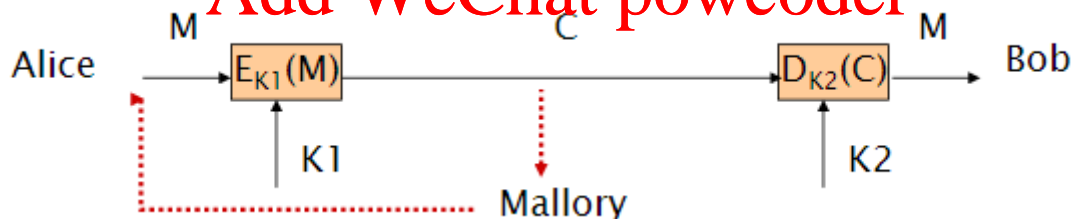
- (a) confidentiality
- (b) integrity
- (c) acceptability
- (d) **availability**

(1.2) Hashing can generally be used to _____ attacks on data integrity.

- (a) mask
- (b) deter
- (c) prevent
- (d) **detect**

(1.3) Which of the following types of cryptanalysis techniques is illustrated/captured in the below figure?

- (a) known plaintext
- (b) **chosen plaintext**
- (c) chosen ciphertext
- (d) chosen text



(1.4) Vigenere Cipher is an example of _____ cipher.

- (a) monoalphabetic substitution
- (b) **polyalphabetic substitution**
- (c) monoalphabetic transposition
- (d) polyalphabetic transposition

(1.5) Which of the following conditions must a public key cryptosystem meet?

- (a) **It must be computationally infeasible to derive the private key from the (respective) public key.**
- (b) It must be computationally infeasible to extract the plaintext by using the public key from the ciphertext which was obtained using the private key.

- (c) It must be computationally infeasible to extract the plaintext by using the private key from the ciphertext which was obtained using the public key.
- (d) It must be computationally easy to encipher or decipher a message given the appropriate key.

(1.6) In the Mintzberg's 10-role managerial model, **Disseminator** role falls in the category of _____ of roles.

- (a) interpersonal
- (b) **informational**
- (c) decisional
- (d) none of the above

Question not applicable!

(1.7) _____ planning focuses on production planning and integrates organizational resources for an intermediate duration (1 – 5 years)

- (a) long-term
- (b) strategic
- (c) operational
- (d) **tactical**

Question not applicable!

Assignment Project Exam Help

(1.8) *Awareness and Training* is a category in the _____ function of the NIST Cybersecurity Framework.

- (a) Identify
- (b) **Protect**
- (c) Detect
- (d) Respond

<https://powcoder.com>

Question not applicable!

Add WeChat powcoder

(1.9) *Anomalies and Events* is a category in the _____ function of the NIST Cybersecurity Framework.

- (a) Identify
- (b) Protect
- (c) **Detect**
- (d) Respond

Question not applicable!

(1.10) When developing a new information security policy, which of the following steps should be taken first (i.e., before others)?

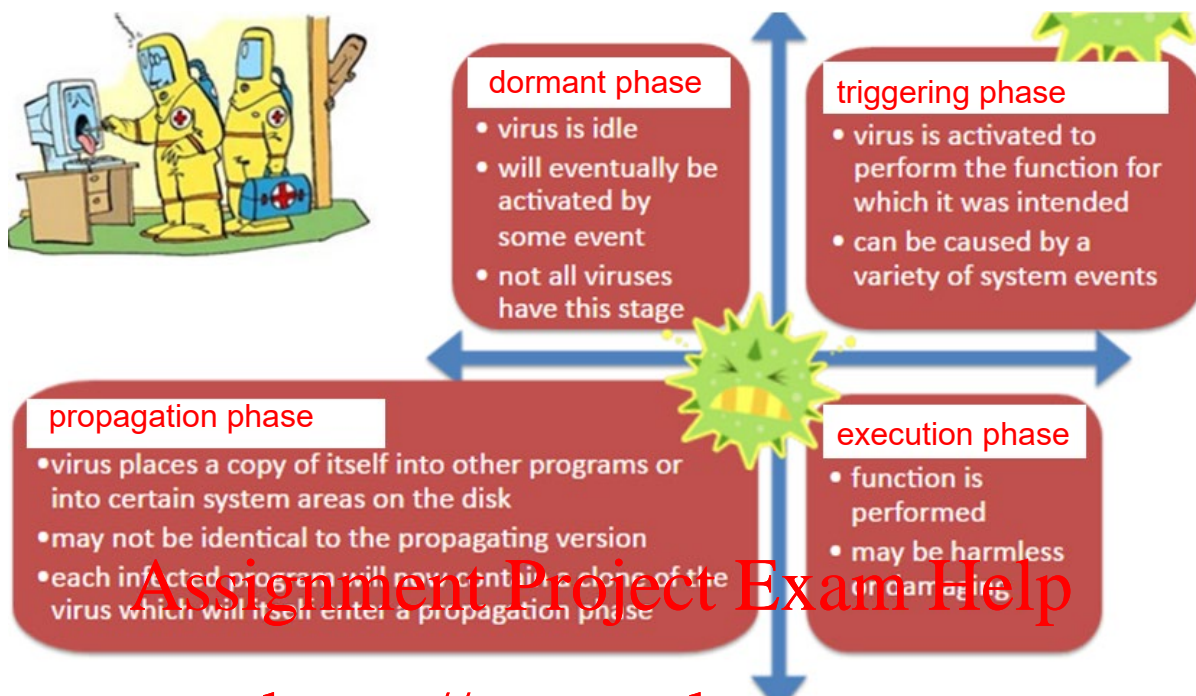
- (a) Obtained all recent/relevant information including those pertaining to the potential impact of the policy on company's risk assessment and IT audit performance.
- (b) **Gain approval from senior management**
- (c) Create a plan on what would be the best approach to distributing the policy.
- (d) Write the policy so that it can be finally presented to the company employees.

Question not applicable!

2. Security Attacks - Potpourri

[12 points]

a) [4 points] The below figure depicts the four phases of a virus lifetime. Complete the figure by filling in the blank spaces with the names of each of the four phases.



<https://powcoder.com>

b) [4 points] What is the main difference between polymorphic and metamorphic viruses? Explain in no more than 2 sentences!

Add WeChat powcoder

Solution:

A polymorphic virus tries to avoid detection by changing (only) its signature (i.e., the bit sequence) with every infection/replication.

A metamorphic virus tries to avoid detection by changing not only its signature but also its actual behavior with every infection/replication.

c) [4 points] In class we have discussed a type of social engineering attack that employs DNS poisoning as a means of its execution. What is the name of this attack? Besides DNS poisoning, what else does the attacker have to 'put in place' for this attack to work?

Solution:

Pharming attack

The attacker also have to create 'spoofed' Web-page(s) that resemble the actual page(s) whose DNS records are contained in the poisoned DNS file. When redirected to these 'spoofed' pages through DNS poisoning, the users should believe that that have accessed the actual/right pages

...

3. Steganography

[10 points]

In order to facilitate the exchange of secret messages, Sally & Harry have developed an image-based steganography system.

After a considerable investigative effort, you have learned that their system deploys an ASCII letter encoding scheme, shown in the below figure. You have also discovered that they use raw RGB images as their 'cover images', and that they embed their secret bits into these images by deploying the LSB scheme. In particular, they use the last 2 bits of each colour channel (in each pixel) for embedding.

This morning, you've seized one of their stego images. The image is of size 20x40 pixels.

Binary	ASCII	Binary	ASCII
000000	A	010000	Q
000001	B	010001	R
000010	C	010010	S
000011	D	010011	T
000100	E	010100	U
000101	F	010101	V
000110	G	010110	W
000111	H	010111	X
001000	I	011000	Y
001001	J	011001	Z
001010	K		
001011	L		
001100	M		
001101	N		
001110	O		
001111	P		

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

a) [6 points] How many secret letters, at most, could be contained in the given image?

Solution:

In RGB images, there are 3 colour channels. Hence, there will be $2 \times 3 = 6$ embedded bits/pixel.

Total # of embedded bits = 20×40 [pixels] \times (2×3) [embedded bits / pixel] = 4,600 [embed. bits]

Max number of secrete letters = $4,600$ [embed. bits] / 6 [bits / letter] = 766 letters.

b) [4 points] Now, assume that instead of using the last 2 bits of each colour channel in a pixel they decide to put all the secret bits into the LSB of only one channel while leaving the other channels intact. (The overall number of secret bits / pixel remains the same as in a.) Would this approach be better or worse than the one originally described? Explain!

Solution:

Putting all 6 secret bits in one color channel would be a worse strategy, as it would introduce a more noticeable distortion of that one colour (due to affecting more significant bits), and ultimately a more noticeable distortion of the entire image. Consequently, this would make the detection/perceptibility of their secret message more likely.

4. Watermarking & Fingerprinting

[10 points]

One way that vendors of digital information try to track and prevent piracy is through the use of digital watermarks. For the purposes of this question, let us assume that it is possible to embed a digital watermark in a document in a such a way that the watermark cannot be removed without destroying the document, and illegitimate copies of the document will never contain a valid watermark.

a) [5 points] One use of digital watermarks is for *usage tracking*. How could a vendor - which possesses a perfect, tamperproof watermark - use this watermark to track any unauthorized usage of their proprietary graphic images (e.g., JPEG images) throughout WWW. Clearly state which functionality the vendor would have to implement (or hire from a third-party company) in order to automate this process.

Solution:

The vendor could deploy a web crawler to search for JPEGs. When one is found, the watermark is extracted and compared to a database of registered images and owners.

b) [2 points] Would your answer under a) constitute a *public watermarking* or *private watermarking* application? Explain!

Solution:

<https://powcoder.com>

In case that the vendor builds and deploys their own web-crawler, it would be a private watermarking application as the watermark key would remain known only to the owner (vendor in this case).

Add WeChat powcoder

In case that the vendor hires third-party web-crawler(s) (e.g., Google), it would be a public watermarking application as the watermark key would have to be given/provided to the third-party web-crawlers ...

c) [3 points] In this particular case, how important the features of 'capacity', 'robustness' and 'imperceptibility' would be for the watermarking algorithm employed? (Circle the answer that you feel is most appropriate in each of the below statements.)

capacity (ability to hide a large number of bits):	very important	not so important
robustness to image manipulation:	very important	not so important
imperceptibility:	very important	not so important

5. Cryptography

[34 points]

5.1 Classic Cryptography [12 points]

Alice and Bob write encrypted messages to each other using a combination of Caesar and Rail Fence cipher. Specifically, each message is first encrypted using Caesar cipher with the key value K , and then such obtained ciphertext is further encrypted using Rail Fence cipher with M rails.

You've managed to seize one of their messages, as shown below. The only think that you know about this message is that it contains exactly one 3-letter word 'the'. The other words are either longer or shorter than 'the'.

zlfxwhbhzo_rth_k_qp_oquhh

Your task is to decrypt the given message, and in doing so to determine the value of K and M that Alice and Bob are using.

Solution:

The first task in decrypting this message is to determine the value of M (# of rails in the Rail Fence algorithm).

We can start by assuming a 2-rail fence, which will give the following:

z		l		f		x		w		h		b		h		z		o				r		t
	h				k																			

By 'decrypting' the given 2-rail fence, we end up with:

zhk_fkz_wqhpb_hozqou_hrht

If 2-rail was indeed used, the above should correspond to the Caesar cipher of the original message. However, clearly, in the above cipher there are 2 3-letter long words, which is a good indication that we are not on the right track. (I.e., a different rail fence should be tried.)

Let us next assume a 3-rail fence, which will give the following:

z				l				f				x				w				h				b
	h		z		o				r		t		h				k				q		p	
						o				q				u				h				h		

By decrypting the given 3-rail fence, we end up with

zh_zloo_frqtxhu_wkh_hqhpb

In this ciphertext there is only one 3-letter sequence, so this is a potentially good candidate for the actual Caesar cipher.

Now, we only have to try to find K that (potentially) mapped 'the' to 'wkh'. Or, find a decryption key that maps 'wkh' to 'the'.

Clearly, with $K=3$ (or decryption key $DK=23$) this mapping is possible.

Consequently, by decrypting the entire message with $DK=23$, we obtain the following plain-text:

we will conquer the enemy

Obviously, the key values that Alice and Bob were using are $K=3$, and $M=3$.

5.3 RSA Cryptography [8 points]

In RSA algorithm, if $p=7$ and $q=13$, what are the five smallest possible numbers for e ?

Solution:

Assignment Project Exam Help

e must be relatively prime (i.e., has no common factors/divisors) to $(p-1)(q-1) = 72$.

72 is divisible by: 2, 3, 4, 6, 8, 9, ...

<https://powcoder.com>


Hence, the first 5 numbers that fit the description for e in this case are: 5, 7, 11, 13, 17.


Add WeChat powcoder

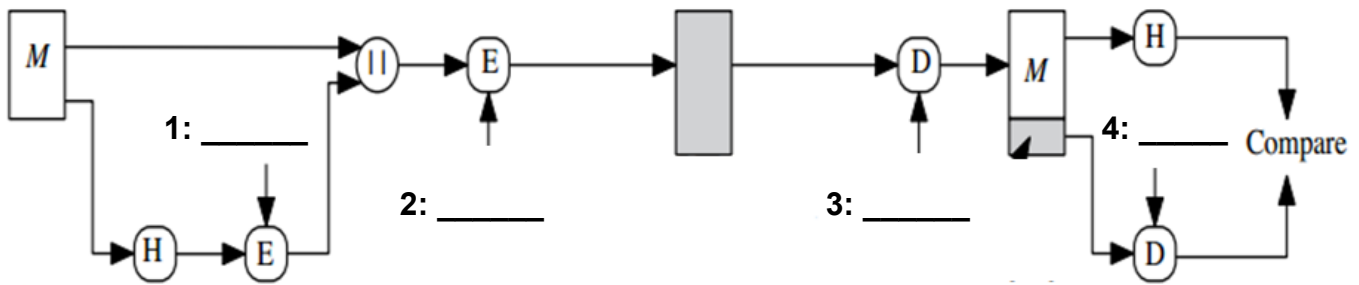
5.3 Public Cryptography in Use [8 points]

In class, we have discussed the below system which can be used for transmission of confidential messages between Bob and Alice as well as for sender authentication.

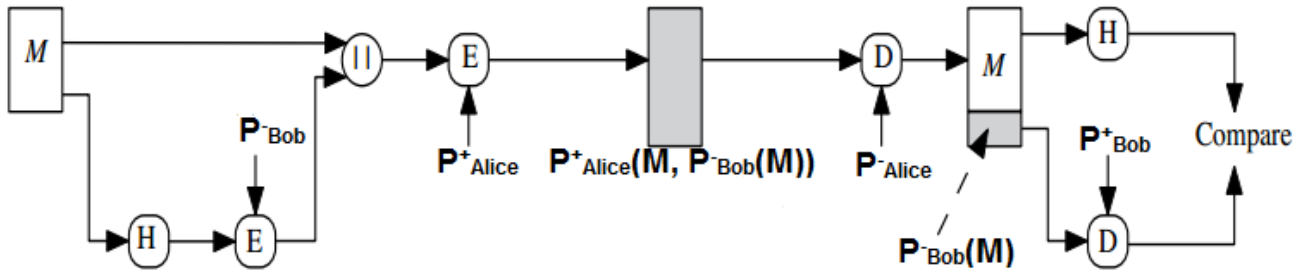
Your task is to specify which particular keys – out of the ones available to Bob and Alice (as indicated in the figure) - should be used in stages 1, 2, 3, and 4 (as indicated in the figure), for this system to function as intended.

 **Bob:**
 P^-_{Bob} , P^+_{Bob} , P^+_{Alice}

 **Alice:**
 P^-_{Alice} , P^+_{Alice} , P^+_{Bob}



Solution:



Assignment Project Exam Help

5.4 Breaking Cryptographic Keys [6 points]

We know that the size of the keyspace has a huge impact on the security of a cryptosystem.

The below table shows the times required to 'crack' RC5 algorithm, when the algorithm employs a key of size 40, 48, 56, and 64 bits respectively. ('Cracking' in this case implies a brute force attack on the actual key. RC5 is a symmetric key block cipher notable for its simplicity.)

- a) [4 points] In the below table fill in the 'keyspace' and 'average number of keys/second' columns.

Key size	Time to find it	Keyspace	Average number of keys/second
40	3.5 hours		
48	313 hours		
56	265 days		
64	1757 days		

Solution:

Key size	Time to find it	Keyspace	Average number of keys/second
40	3.5 hours	2^{40}	8.7×10^7
48	313 hours	2^{48}	2.5×10^8
56	265 days	2^{56}	3.14×10^9
64	1757 days	2^{64}	1.21×10^{11}

- b) [2 points] By studying the provided table, can you characterize the growth in complexity of cracking RC5 as the key size increases? (For example, does the cracking complexity have a linear or exponential growth?)

Solution:

Clearly exponential!

Assignment Project Exam Help

<https://powcoder.com>

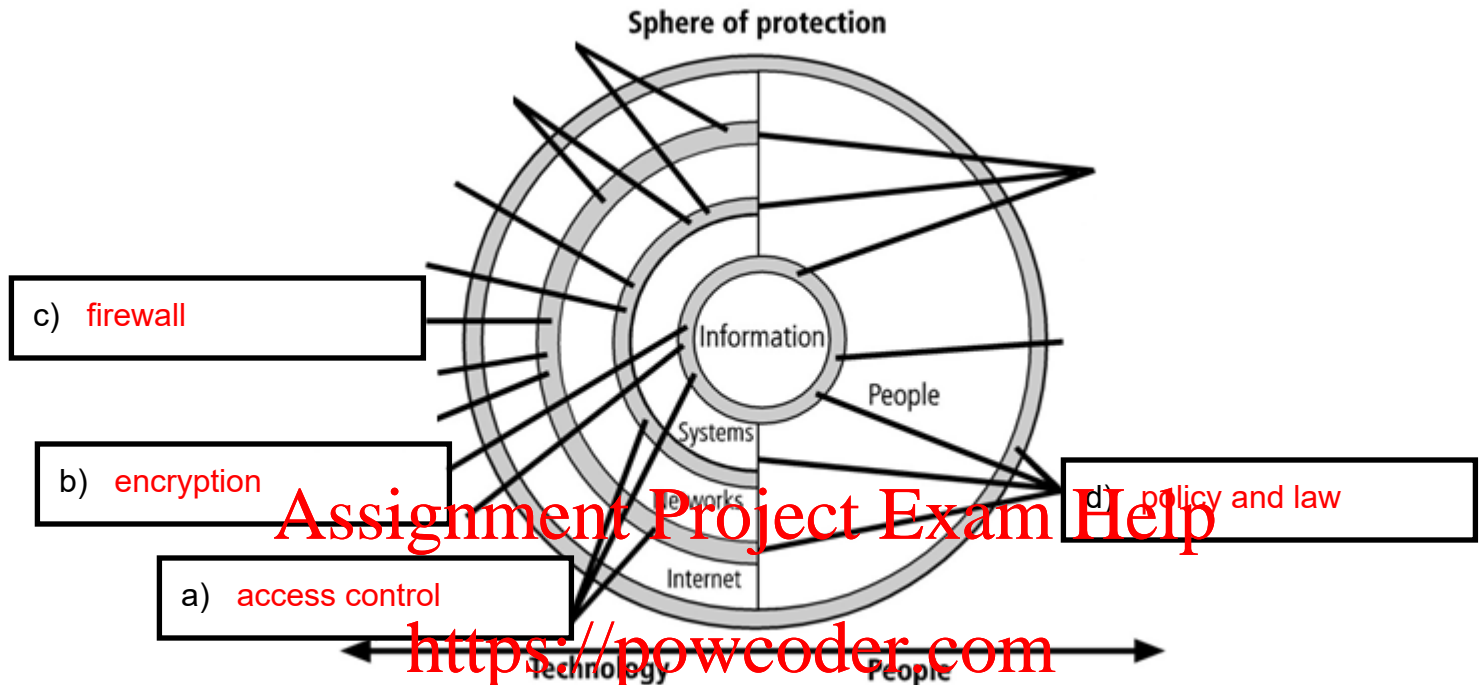
Add WeChat powcoder

6. Access Control Pottpouri

[14 points]

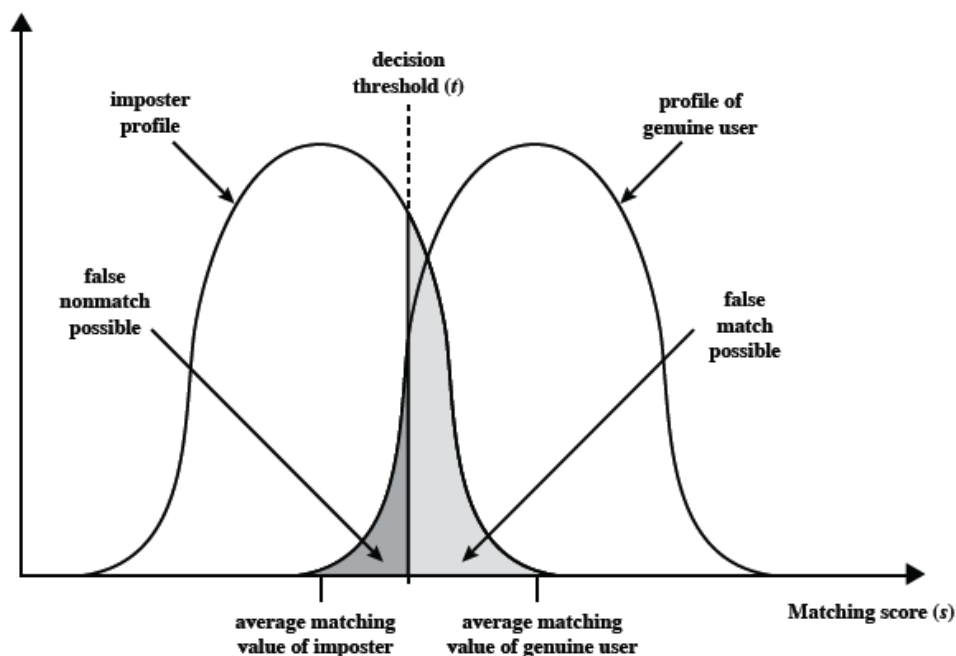
6.1 Spheres of protection [8 points]

In class, we have discussed the *Layered Model of Information Use and Protection*. In the below figure, specify the names of protective technologies that you think best correspond to a) to d).



6.2 Biometric detection [6 points]

In class, we have discussed how the change in the 'decision threshold' can impact the performance of a biometric system.



By referring to the above figure, your task is to complete the following two sentences so that they correctly capture the impact of changing the system's decision threshold on the system's False Accept/Match and False Reject/Nonmatch rates.

As the decision threshold increases and the system becomes more sensitive, the system's False Accept Rate _____ **decreases** _____ .

As the decision threshold decreases and the system becomes less sensitive, the system's False Reject Rate _____ **decreases** _____ .

(Complete the above sentences by choosing either 'increases' or 'decreases'.)

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder