



Department of Computer Science and Engineering

CSE 3482: Introduction to Computer Security

Instructor: N. Vljic

Final Examination

Instructions:

- Examination time: 180 min.
- Print your name and CSE student number in the space provided below.
- This examination is closed book and closed notes.
- There are 8 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.

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

FIRST NAME: _____

LAST NAME: _____

STUDENT #: _____

Question	Points
1	/ 20
2	/ 10
3	/ 20
4	/ 8
5	/ 10
6	/ 10
7	/ 11
8	/ 11
Total	/ 100

1. Multiple Choice

[20 points]

Circle the correct answer(s) for the following statements.

(1.1) Assume Bob leaves himself logged onto Facebook on his mobile phone. Alice gets hold of Bob's phone, and changes his Facebook password. This action will constitute a violation of which of the following:

- (a) data confidentiality
- (b) data integrity
- (c) data availability
- (d) none of the above

(1.2) A zero-day attack that exploits a particular vulnerability will stop being a 'zero-day' attacks once _____.

- (a) the vendor discovers (i.e., becomes aware) of the given vulnerability
- (b) the vendor discloses this vulnerability publicly
- (c) patch for the vulnerability is released
- (d) patch deployment is completed

(1.3) Triple-DES algorithm applies the standard DES encryption/decryption 3 times, using the same or different keys (K1, K2, K3). Which of the following Triple-DES keying options results in the strongest (i.e., hardest to 'break') encryption?

- (a) All three keys are independent.
- (b) $K1 \neq K2$, and $K1 = K3$.
- (c) $K1 = K2$, and $K1 \neq K3$.
- (d) All three keys are the same.

(1.4) Public Key algorithms are:

- (a) two times faster than Secret Key algorithms
- (b) two times slower than Secret Key algorithms
- (c) 1,000 to 10,000 times faster than Secret Key algorithms
- (d) 1,000 to 10,000 times slower than Secret Key algorithms

(1.5) What is the function of an enterprise/corporate information security policy?

- (a) Issue enterprise/corporate standard to be used when addressing specific security problems.
- (b) Issue guidelines in selecting equipment, configuration, design, and secure operations.
- (c) Define the main security objectives and the most appropriate security framework required to meet the key business objectives.
- (d) Define the specific assets to be protected and identify the specific tasks which must be completed to secure these assets.

Question not applicable!

(1.6) In the life-cycle of a security policy, *policy distribution* stage ensures that

- (a) general support from the senior management is obtained
- (b) the policy is written in a way that all employees can read and comprehend it
- (c) the policy is uniformly enforced across the entire organization
- (d) none of the above

Question not applicable!

(1.7) In cases when a biometric system is used for the purposes of user identification, whenever a new user attempts to validate himself to/through this system, the user's profile will be compared against _____.other profile(s) stored in the system's database.

- (a) no
- (b) one
- (c) a few
- (d) all

(1.8) You are comparing biometric systems. Security is the top priority. A low _____ is most important in this regard.

- (a) FAR
- (b) FRR
- (c) ERR
- (d) MTBF

Assignment Project Exam Help

<https://powcoder.com>

(1.9) Salting passwords help security in which way?

- (a) Make passwords easier to remember.
- (b) Make passwords easier to store.
- (c) Deter online password attacks.
- (d) Deter offline password cracking.

Add WeChat powcoder

(1.10) Which of the following are correct definitions?

- i) *Brute force attacks* – Performed with tolls that cycle through many possible character, number, and symbol combinations to uncover a password.
- ii) *Dictionary attacks* – Files of thousands of words are compared to the user's password until a match is found.
- iii) *Social engineering* – An attacker falsely convinces an individual that they have the necessary authorization to access specific resources.
- iv) *Rainbow table* – An attacker uses a table that contains all possible passwords already in a hash format.

- (a) i, ii
- (b) i, ii, iv
- (c) i, ii, iii, iv
- (d) i, ii, iii

(1.11) An access control system that requires its users to provide/enter one password and one PIN-number is an example of:

- (a) one-factor authentication system
- (b) two-factor authentication system
- (c) bi-factor authentication system
- (d) none of the above

(1.12) According to NIST Cybersecurity Framework, Risk Management is a subcategory of _____ function.

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

Question not applicable!

(1.13) Which of the following is not true with respect to qualitative risk analysis?

- (a) it relies on expert experience
- (b) it uses labels to categorize threats based on their likelihood and impact
- (c) it results in concrete probability percentages
- (d) all of the above are correct

Question not applicable!

Assignment Project Exam Help

(1.14) What would be the Annualized Rate of Occurrence (ARO) where a company employs 100 data entry clerks, each of whom averages one input error per month?

- (a) 100
- (b) 120
- (c) 1,000
- (d) 1,200

<https://powcoder.com>

Add WeChat powcoder

(1.15) For a vulnerability that is 'high cost' and 'exceptionally low risk', which of the following controls would be most appropriate:

- (a) acceptance
- (b) avoidance
- (c) transference
- (d) none of the above

(1.16) A TCP-SYN flood exhausts what resources at its target?

- (a) bandwidth-related resources
- (b) application-related resources
- (c) processing-related resources
- (d) none of the above

Question not applicable!

(1.17) In the Common Law legal system, judges play a/an _____ role.

- (a) active and creative
- (b) passive and technical
- (c) completely irrelevant
- (d) none of the above

Question not applicable!

(1.18) Which of the following are subcategories of Public Law?

- (a) Family Law
- (b) Contract Law
- (c) Administrative Law
- (d) Property Law

Question not applicable!

(1.19) _____ is a category of Law that seeks to provide compensation for people who have suffered harm from wrongful but non-intentional acts of others.

- (a) Criminal Law
- (b) Compensation Law
- (c) Constitutional Law
- (d) Tort Law

Question not applicable!

(1.20) In the USA, _____ Act aims to protect confidentiality and security of health-related data.

- (a) CFAA
- (b) HIPAA
- (c) Gramm-Leach-Bliley
- (d) COPI

Question not applicable!

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

2. Steganography

[10 points]

In order to facilitate the exchange of secret messages, Gru and Dr. Nefario have developed an image-based steganography system. After a considerable investigative effort, you have learned that their system deploys a *semi-random bit-hiding scheme*. In particular, the secret bits are semi-randomly scattered inside the bit-sequence that corresponds to (can be generated from) a provided stego image. Their stego images are designed to look like an $n \times n$ matrix of different-coloured blocks (see Figure 3). To extract the actual secret message from one of such stego images, the following procedure should be followed:



Step 1) The coloured block-matrix of each particular stego image is 'scanned' row-by-row (top row first) left-to-right, and each encountered colour is decoded using the scheme shown in Figure 2. Hence, the output of this step is a bit sequence which we annotate as *BiSe sequence*.

Step 2) The actual secret message is comprised of only (some) select bits of *BiSe sequence*. The location of these bits can be identified by means of a 'key' that gets exchanged together with the respective stego image. We will annotate these special/select bits of *BiSe sequence* as *SeBi bits*.









Step 3) To convert *SeBi bits* into English-language text, the encoding scheme shown in Figure 1 is used.

This morning, you've seized an email exchange from Dr. Nefario to Gru. The email contained a stego image (the one shown in Figure 3), and the following sequence of numbers:

2 3 5 7 9 13 18 20 21 23 24 28 29 33 34 35 37 38 40 41 43 44 45
46 47 48 51 52 55 57 59 61 66 68 70 71

Binary	ASCII
000000	A
000001	B
000010	C
000011	D
000100	E
000101	F
000110	G
000111	H
001000	I
001001	J
001010	K
001011	L
001100	M
001101	N
001110	O
001111	P

Binary	ASCII
010000	Q
010001	R
010010	S
010011	T
010100	U
010101	V
010110	W
010111	X
011000	Y
011001	Z

	00110011
	00001111
	10101010
	11100111
	11001100
	11110000
	01010101
	00011000

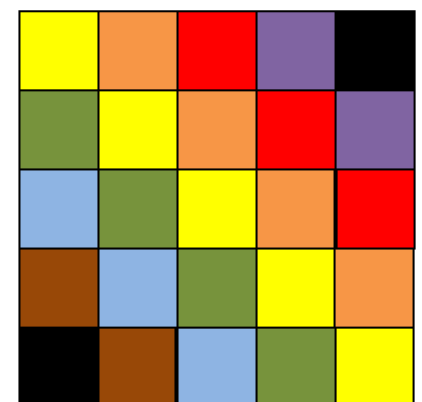


Figure 3

Figure 2

Figure 1

What is the content of their message?

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

3. Encryption Potpourri

[20 points]

3.1 Classic Encryption

(a) Vigenere Cipher [6 points]

Use the Vigenere cipher to decrypt “YHPRWELEUUXAPIY” with the key “FALL”. Vigenere table is given below.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

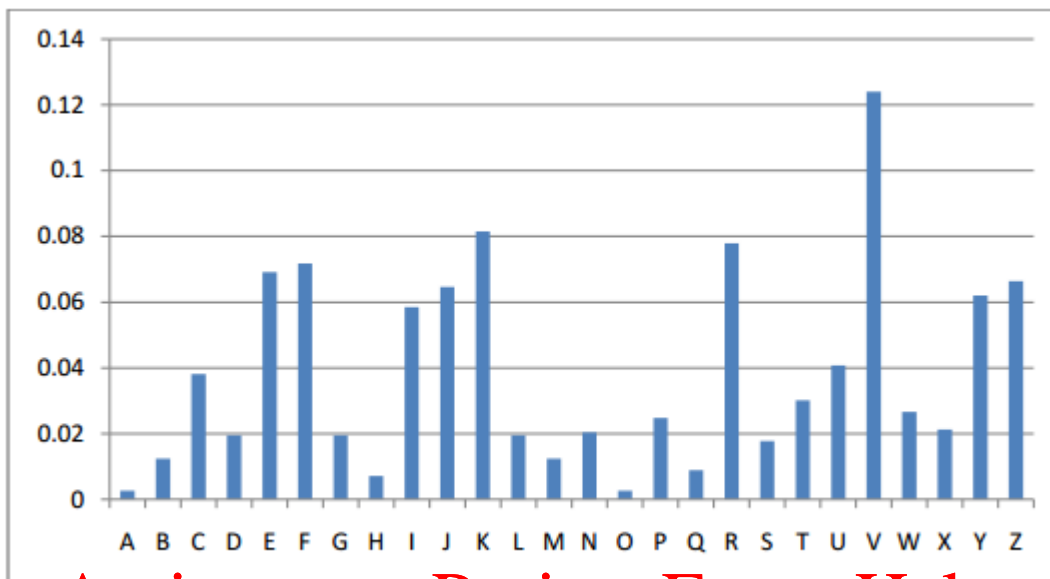
Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

(b) Simple Substitution Cipher [6 points]

A long message was encrypted with a simple substitution cipher (think of Caesar Cipher). Its frequency analysis reveals the following probability distribution:



Assignment Project Exam Help

Use this information to decrypt the following portion of the message:

<https://powcoder.com>

T	F	E	W	Z	U	V	E	K	Z	R	C

Add WeChat powcoder

3.2 Public Encryption

(a) Diffie-Hellman algorithm [4 points]

Suppose Alice and Bob wish to do Diffie-Hellman key exchange. Alice and Bob have agreed upon a prime $p=13$, and a generator $g=2$. Alice has chosen her private exponent to be $a=5$, while Bob has chosen his private exponent to be $b=4$.

Show the intermediate quantities that both Alice and Bob calculate, as well as the final shared secret that Diffie-Hellman produces.

Assignment Project Exam Help

<https://powcoder.com>

(b) Digital Signature [4 points]

A new web service SignMe allows people to sign their web pages. (Pages could be hosted anywhere in the WWW.) All the service does is append a special hidden HTML tag at the bottom of an otherwise normal web page. The tag contains the author's name, the date, and a signature. (The signature contains the author's name and date signed by the author's RSA private key). The web page itself is unencrypted, but the signature can be validated by going to <http://www.signme.com/keys.html> (which contains a list of all registered SignMe users and each user's public key) to retrieve the author's public key.

Now, assume Bill Gates is a user of this service. What exactly would take for an attacker to make it appear that Bill Gates has put up a signed web page somewhere in the WWW with the content "I am closing my shop today, and will start working for Linux tomorrow"? (I.e., briefly outline the steps needed to accomplish such an attack.)

4. Hashing

[8 points]

An Internet radio station wishes to broadcast streamed music to its subscribers. Non-subscribers should not be able to listen in. When a person subscribes to the station, she is given a software player with a number of secret keys embedded in it. The radio station encrypts the broadcast content using a special AES key K , which periodically changes.

Now, the secret keys in each legitimate player can be used to derive K and (at the same time) enable legitimate subscribers to tune in. Namely, when a subscriber cancels her subscription, the radio station will encrypt the future broadcast using a new key K' . All valid players will be informed of the cancelled subscription (as a part of the broadcast) and will be able to derive the new K' , while the canceled subscriber should no longer be able to derive K' .

Suppose that the total number of potential subscribers is less than $n=10^5$. Let R_1, R_2, \dots, R_n be 512-bit random values. The player shipped to a subscriber number k contains all the R_i -s except for R_k - i.e., the player contains 99999 keys (except 'its own'). Let S be the set of currently subscribed users. Show that the radio station can construct a key K used to encrypt the broadcast content in a way that any subscriber in S can re-derive K (from the R_i -s in her player) while any subscriber outside of S cannot derive K . You may assume that the set S - identity of currently subscribed users - is indirectly known to everyone at all times (again, due to additional broadcast information).

Hint: consider using one-way hash function for the purposes of constructing the AES key.

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

5. Access Control

[10 points]

5.1 Biometrics [6 points]

A biometric identification scheme usually has a threshold parameter T such that increasing T makes it harder to pass, and decreasing T makes it easier. The *false accept rate* $FAR(T)$ decreases with increasing T , while the *false reject rate* $FRR(T)$ increases.

Now, assume a system where T is a value in the range $[0, 1]$, and FAR and FRR change according to:

$$FAR(T) [\%] = 50 - 48 \cdot T$$

$$FRR(T) [\%] = 4 + 7.2 \cdot T$$

Furthermore, assume the system is set to operate in a mode that achieves a balance between FAR and FRR .

In March 2020, this system has performed 7000 authentications. How many of these authentications/users have been falsely rejected from accessing the system?

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

5.2 Access Control Models [4 points]

Complete the following two sentences:

Bell-LaPadula and Biba models are examples (i.e., special cases) of _____ access control. (Choose from: MAC, DAC, RBAC.)

Question not applicable!

In Biba model a subject S is granted *read* access to object O only if S 's access level is _____ than that of O . (Choose from: HIGHER, LOWER.)

6. Password Cracking

[10 points]

The 26 lower-case letters of the alphabet and the digits 0, 1, 2, ..., 9 are used to make four-character long computer passwords.

6.1 [3 points]

How many passwords are possible if repetition of characters within a password is not allowed?

Assignment Project Exam Help

6.2 [7 points]

How many passwords are possible if repetition of characters within a password is allowed, BUT passwords must contain at least one letter and at least one digit?

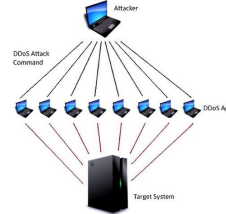
<https://powcoder.com>
Add WeChat powcoder

7. Risk Management

[11 points]

Flowers, E-Shop, DDoS, Akamai

You own an online store that sells and ships flowers within GTA. Your sales average \$600 a day. You are worried about being targeted by a Distributed Denial of Service (DDoS) attacker with the aim of extortion. Such an attack would completely bring down your website, and you do not have any alternative way of doing business.



You have heard that, if you become a victim of a DDoS attack, the attacker will require on average \$1,500 to stop the attack. Once the money is received, the attack will stop within a day. Otherwise, it will continue for 7 days. Based on past data, you estimate that there is 0.1% chance that DDoS attackers target your small site any particular day. (I.e., 1 out of 1000 small businesses is DDoS-ed every day.)

The company Akamai offers you a distributed hosting service that reduces the chances of success for such attacks to 20% (otherwise the attackers definitely succeed). Akamai requires an annual premium of \$400 for this service.

Assignment Project Exam Help

<https://powcoder.com>

7.1 [3 points]

Compute the annual loss expectancy for the DDoS attack, assuming you do nothing.

Add WeChat powcoder

7.2 [7 points]

Now, suppose you are considering to deploy one of the following two control strategies in the coming year.

Strategy 1: If the attack occurs, pay money to the attackers (you do not care about legal consequences, and are willing to pay the ransom right away).

Strategy 2: Buy the Akamai service; but in case an attack succeeds, do not pay attackers any money.

Calculate the NRRB for each strategy. Which strategy would you recommend?

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

7.3 [1 points]

The strategy that you are recommending in (b) is an example of:

- (i) Risk acceptance
- (ii) Risk avoidance
- (iii) Risk transference
- (iv) Risk mitigation

Circle the right answer.

8. DDoS Potpourri

[11 points]

8.1 [3 points] Amplified Reflector Attack

In class we have discussed the concept of amplified reflector DDoS attack (see below figure).



Assume a company wants to ensure that their machines are never used as reflectors in an amplified reflector DDoS attack. What is the first step/measure that the company should take in order to achieve this objective?

Question not applicable

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

8.2 [4 points] Botnet Architecture

Internet Service Providers (ISPs) could potentially play an important role in preventing and defending against DDoS attacks. Name two different measures that ISPs could take in order to:

- 1) stop an ongoing (e.g., reflector) DDoS attack?
- 2) prevent any DDoS attack from even starting?

8.3 [4 points] DNS DDoS Attack

The web server of a company called ABCSecurity has come under a massive DDoS attack. The attackers are using DNS amplification: they identified several third-party DNS servers that will respond to any DNS query, and they are sending many spoofed DNS queries to those DNS servers. In particular, each DNS query is sent in a spoofed UDP (i.e., IP) packet, where the source IP address is forged to be that of ABCSecurity's server. Also, each query has been chosen so that it will trigger a response that is much larger than the query itself, thus amplifying the effect of the attack.

Consider the packets that ABCSecurity's server has received as a result of this DNS amplification attack. For each of the following fields in the IP header, state whether you expect the field to be the same for all these attack packets or to differ from packet to packet (circle one choice). If you select 'same', describe the value of that field in the space to the right. If you select 'differs', also briefly justify your answer, in the space to the right.

SOURCE ADDRESS:

(a) SAME

(b) DIFFERS

Question not applicable!

Assignment Project Exam Help

DESTINATION ADDRESS:

(a) SAME

(b) DIFFERS

<https://powcoder.com>

Add WeChat powcoder