NATIONAL UNIVERSITY
of Computer & Emerging Sciences, Lahore

Department of Computer Science

CS411 – Network Security
Feb 6th 2020
Quiz 1 – Weight 3.33 % - total points 41
Student Name ________________________________Student ID___________________________

Any kind of dishonesty will lead to an F in this quiz (as a minimum penalty)

Q1. Consider a scenario where you open your flex account but are not able to see your complete/correct attendance although the instructor can see the complete/correct attendance. Which kind of security violation is this? (Three word answer required) (1 point)

Integrity of data.

Q2. Consider a scenario where you open your flex account and also able to see the page that used by the instructors to provide comments about the course to the HOD. The page is currently empty. Which kind of security violation is this? (Three word answer required) (1 point)

Confidentiality of service.

Q3. What is the relationship between an attacker and an attack? (One word answer required) (1 point)

Launches (or its synonyms)

Q4. What is the relationship between a vulnerability and a security requirement? (One word answer required) (1 point)

Avoids/mitigates/secures/removes (or synonyms)

Q4. Consider a scenario where you open your flex account but are also able to see other peoples' grades. Which kind of security violation is this? (Three word answer required) (1 point)

Confidentiality of data.

Q6. What are the two conditions for any encryption scheme to be computationally secure? (2 points)

(1) the cost of breaking the cipher exceeds the value of the encrypted information, and

(2) the time required to break the cipher exceeds the useful lifetime of the information.

Q7. Consider a scenario where try to log in to your flex account but are unable to due to a large number of students who are already logged in. Which kind of security violation is this? (Three word answer required) (1 point)

Availability of service.

Q8. What are the two problems with one-time-pad encryption? (2 points)

1. There is the practical problem of making large quantities of random keys. Any heavily used system might require millions of random characters on a regular basis. Supplying truly random characters in this volume is a significant task.

2. Even more daunting is the problem of key distribution and protection. For every message to be sent, a key of equal length is needed by both sender and receiver. Thus, a mammoth key distribution problem exists.

Q9. Consider a scenario where you are being sent spam via email, SMS, etc. Which is the most expensive asset of yours that is being attacked? (One word answer required) (1 point)

Time

Q10. What is the relationship between an attack and a vulnerability? (One word answer required) (1 point)

Exploits (or its synonyms)

Q11. Suppose that you wrote a program which does not free memory (because you did not know that it could be an issue) after it is finished using it. Suppose this program is run on a server. With time, the server starts getting out of memory messages and crashes. Who is the attacker here? (1 point)

No one

Q12. How many keys are required for two people to communicate via a cipher? (2 points)

One key for symmetric and two keys for asymmetric

Q13. What are the two main approaches we have studied to crack cipertext? (2 points)

Cyptanalysis and brute force (or synonyms)

NATIONAL UNIVERSITY
of Computer & Emerging Sciences, Lahore

Department of Computer Science

CS411 – Network Security
Feb 6th 2020
Quiz 1 – Weight 3.33 % Quiz 1 – Weight 3.33 % - total points 41
Student Name ________________________________Student ID___________________________

Any kind of dishonesty will lead to an F in this quiz (as a minimum penalty)

Q14 a. Use the following two matrices to encrypt "Must see you over Cadogan West. Coming at once" (4+4 points)

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

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

UZTBDLGZPNNWLGTGTUEROVLDBDUHFPERHWQSRZ

UZTBDLGZPNNWLGTGTUEROVLDBDUHFPERHWQSRZ

Q14 b. How can you explain the results? (4 points)

A cyclic rotation of rows and/or columns leads to equivalent substitutions. In this case, the second matrix is obtained from the first matrix by rotating the columns by one step and the rows by three steps.

Q15. Construct a playfair matrix with the key **OCCURRENCE**. (2 points)

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

Q16. How many possible keys can a playfair cipher have? Ignore the fact that some keys may have identical results. (4 points)

25! Or 2^{84}

Q17. How many UNIQUE keys can a playfair cipher have? (4 points)

24!

Q18.Construct a playfair matrix with the key **LARGEST**. (2 points)

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