CSC668 MIDTERM

NAME STUDENT ID

Email to: nazila@globaltechnologies.biz

1: What are digital certificates used for and who issues them? (10)

2: What is a digital signature and what are its main properties? (10)

3 Two bytes are known to have been encrypted by the same 8-bit RC4 stream producing C1 = 1111 0011 and C2 = 1111 1001 respectively. The bytes are believed to be non-capitalised vowels 'a':61(Hex) 'e':65, 'i':69, 'o':6F 'u':75. What are they? What is the 8 bit key? (10)

4. Why is WEP not considered as a good security solution for WLANs and what are the main improvements of more recent standards (namely 802.11X and 802.11i)? (10)

5. estimate the amount of time it would take to crack a DES encryption by testing all possibilities? If you have a 1GHZ processor, could you estimate the amount of time it would take to crack a DES encryption by testing all 2^56 possibilities? (10)

Assuming:

2^56 keys

200 cycles to go through each iteration

1 Ghz Machine

Completion

Complete each statement.

6. A(n) _____ site has all the equipment needed for an organization to continue running, including office space and furniture, telephone jacks, computer equipment, and a live telecommunications link.

7. The term ___information security ref. 9_____ is frequently used to describe the tasks of guarding information that is in a digital format. (5)

8. A(n) ___scanning ref 39_____ acts as the central base station for the wireless network. (5)

9. A wireless device is set to look for beacon frames from the AP. This is known as _____google phishing ref 57_____. (5)

10. In WEP, RC4 uses a(n) _____ to create the keystream. (5)

Matching (25 total)

Match each item with an statement below:

a.	Security	f.	The FCC
b.	Distributed attacks	g.	Unregulated bands
c.	Firewalls	h.	IEEE 802.11n
d.	IEEE	i.	AreTec
e.	IEEE 802.11u		

_____ 11. restrict specific types of malware from entering a network. (4)

_____ 12. greatest disadvantage to wireless LANs. (4)

_____ 13. standards for how WLANs connect to external networks such as the Internet or cellular networks. (4)

_____ 14. the world's largest technical professional society with members around the globe. (4)

_____ 15. bands of the radio spectrum that are available nationwide to all users, without requiring a license. (3)

_____ 16. factor that makes security increasingly difficult. (3)

_____ 17. organization that promotes standardization in wireless technologies. (3)