

# Computer and Network Security

## Fall Semester 2002

### Quiz No. 5

October 29, 2002

Time Allowed: 20 Minutes

Name: SOLUTION

Total: 40 Points (2 Points Each)

Circle the letter corresponding to the correct answer.

1. A Mixed Linear Congruential Random Number Generator is described by the equation:

$$X_{i+1} = (aX_i + c) \bmod m$$

For the following values of  $a=3$ ,  $c=4$ ,  $m=20$ , and  $X_0=5$ , what will be the value of  $X_3$ ?

- a. 19      b. 1      c. 7      d. None of the other given choices

2. An Additive Congruential Random Number Generator requires a sequence of  $n$  numbers  $X_1, X_2, \dots, X_n$  and produces an extension of the sequence using the relationship:

$$X_i = (X_{i-1} + X_{i-n}) \bmod m, i = n+1$$

For the original sequence  $\{X_1=7, X_2=9, X_3=2, X_4=5, X_5=6\}$ ,  $n=5$ ,  $m=10$ , what will be the value of  $X_7$ ?

- a. 1      b. 2      c. 3      d. None of the other given choices

3. Given the Mid-Square Method of four digit random integer generation and the seed value of  $X_0=9876$ , the value of  $X_2$  would be:

- a. 5353      b. 6546      c. 9776      d. None of the other given choices

4. In the IPSec protocol the AH service does not provide which of the following features?

- a. Confidentiality      b. Data Origin Authentication      c. Rejection of replayed packets      d. Connectionless Integrity

5. This operating system has a built-in kernel level packet filter and circuit level gateway firewall.

- a. Linux      b. Windows NT      c. Both      d. None

6. A destructive program that has been disguised (or concealed in) an innocuous piece of software is called:

- a. Worm      b. Virus      c. Trojan Horse      d. Bacteria

7. Malicious code which replicates itself without limit to exhaust a resource is called:

- a. Trojan Horse      b. Time Bomb      c. Rabbit      d. Backdoor

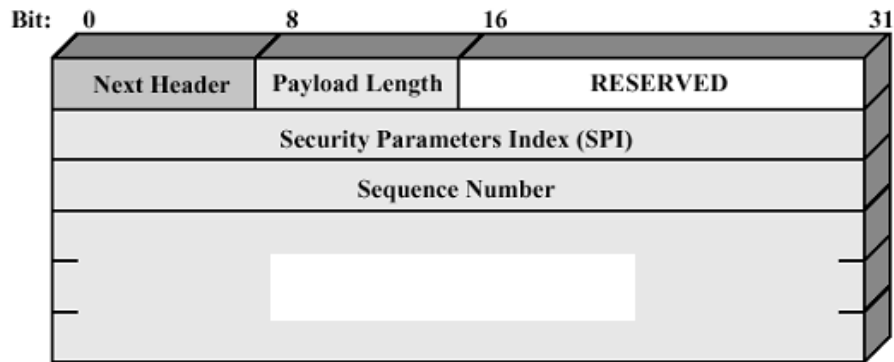
8. Viruses which attempt to hide their presence are called:

- a. Macro Viruses      b. Polymorphic Viruses      c. Multipartite Viruses      d. Stealth Viruses

9. On a standard UNIX/Linux system this file contains the warning message which is displayed before the user is presented with the login prompt.

- a. /etc/passwd      b. /etc/nologin      c. /etc/issue      d. /etc/securetty

10. Shown below is the header format for the IPSec Authentication Header. What is the name of the field following the Sequence Number field?



- a. *Window Size*    **b. *Authentication Data***    c. *Initialization Vector*    d. *Padding*

11. Proxy servers are application specific.

- a. *True***    b. *False*

12. A system or group of systems that enforces an access control policy between two networks is:

- a. *Relay*    b. *Repeater*    c. *Hub*    **d. *Firewall***

13. A PRNG by itself will be insecure without a TRNG for seeding.

- a. *True***    b. *False*

14. Which of the following types of firewalls is transparent to users?

- a. *Proxy Server*    **b. *Packet Filter***    c. *Packet Server*    d. *Proxy Filter*

15. This type of backup includes all files that were created or modified since last Full backup. The Archive Bit is not reset.

- a. *Full Copy Backup*    **b. *Differential Backup***    c. *Incremental backup*    d. *Exponential Backup*

16. This type of backup would require only a single tape to restore the system.

- a. *Full Backup***    b. *Differential Backup*    c. *Incremental backup*    d. *Exponential Backup*

17. The Mean Time Between Failure (MTBF) of an array of hard disks will be higher than the MTBF of an individual drive in the array.

- a. *True*    **b. *False***

18. RAID-5 arrays provide greater storage efficiency than RAID-1 arrays.

- a. *True***    b. *False*

19. Shadow password system stores passwords in the file /etc/shadow which is world-readable

- a. *True*    **b. *False***

20. Sometimes the electrical power level dips quite a bit below normal, this can be caused by a sudden surge in power demand, e.g. on a hot day when everybody turns on their air conditioners. This dip is called a

- a. *Black out*    b. *Surge*    **c. *Brown out***    d. *Double conversion*