# CSCI 604 Distributed Computer Systems Architecture

# Unit 5

|  |  |  |
| --- | --- | --- |
| Teacher: | George Rudolph |  |
| Subject: | Distributed Systems Security and Distributed File Systems |  |
| Objective 1: | Security techniques |  |
| Objective 2: | Cryptographic algorithms |  |
| Objective 3: | Digital signatures |  |
| Objective 4: | File Services, with case studies |  |

## C Level Maximum 50 points

Remember that C-level questions are ideally designed for oral defense. Your written answers may include pictures, drawings, short phrases instead of sentences, as long as the answer is clear and says what you mean.

1. Describe two physical security policies in the organization where you work or attend school. (5pts)
2. PGP is often used for secure email. Create a flyer that describes the steps two users must take to use PGP for secure email. (10 pts)
3. The TEA algorithm given in Figures 11.7-11.9 of your text is not portable to all machine architectures. Explain why. How could a message that is encrypted by this algorithm be transmitted so that it can be decrypted on any architecture? (10 pts)
4. Modify the TEA program of Figure 11.9 to use cipher block chaining (CBC). Pseudocode is sufficient.(10 pts)
5. (You cannot do this one and #6) Construct a stream cipher application based on the algorithm in Figure 11.9. Pseudocode is sufficient. (10 pts)
6. In the Needham-Schroeder authentication protocol authentication protocol with secret keys, explain why the following version of message 5 is not secure. (10 pts)   
   A -> B: {NB}KAB
7. List 5 solutions to the problems with 802.11 WEP as discussed in your text. (5 pts)
8. Explain why the RPC interface to early NFS implementations is potentially insecure. NFS 3 closed this loophole using encryption. How is the key kept secret? Is the security of the key adequate? (10 pts)
9. What data must the NFS client module hold for each user-level process? (5 pts)
10. How does the NFS automounter help improve the performance and scalability of NFS? Is automounter secure? (5pts)
11. How many lookup calls are needed to resolve a five-part pathname (like /usr/users/harryp/code/myfile.cpp) for a file stored on an NFS server? Why is the translation performed step-by-step?

## B Level 30 points—Choose Two

1. Estimate the time it takes to crack a 56-bit DES key by brute-force using a 200MIPS computer. Assume the inner loop for a brute-force attack uses 10 instructions per key value, plus the time to encrypt an 8-bit plaintext (see Figure 11.13). Perform the same time calculation for a 128-bit IDEA key. Extrapolate to estimate the cracking time for a 200,000 MIPS parallel processor.
2. Find benchmark implementations of the algorithms listed in Figure 11.13, run them on your own laptop and compare results with those in Figure 11.13.
3. Implement the TEA algorithm and one other algorithm that you choose, in Java. Benchmark your (two) implementations and compare the results against the ones in Figure 11.13.
4. Decrypt the following message using frequency analysis. You have to figure out the cipher, no decryption tools allowed. Note: Interior spaces are included in the message.

XSDFIDSVDRSXDXSDFIDXLEXDMWDXLIDUYIWXMSR

LIXLIVDXMWDRSFPIVDMRDXLIDQMRHDXSDWYJJIV

XLIDWPMRKWDERHDEVVS WDSJDSYXVEKISYWDJSVXYRI

SVDXSDXEOIDEVQWDEKEMRWXDEDWIEDSJDXVSYFPIW

ERHDFBDSTTSWMRKDIRHDXLIQ

## A Level 20 points—Choose One

1. Should export of cryptographic technology be controlled by the US government?
2. Recently Blizzard restricted access to World of Warcraft game servers to players in Iran, in compliance with newly-imposed technology export restrictions. What security concerns are involved in that blockade? Do you think that kind of blockade is fair? Do you think it does what it intends?
3. Do you think encryption software should include secret loopholes, trapdoors or backdoors? Is this an effective way to retain control of a technology, or the results it produces?
4. Compare the features of AFS and NFS, with emphasis on scalablity. Which recent developments, if any, offer enhanced scalability?

F: < 60 D: < 70 C: < 80 B: < 90 A: >= 90