* **1.3**Consider a desktop publishing system used to produce documents for various organizations.
  1. **Give an example of a type of publication for which confidentiality of the stored data is the most important requirement.**

**ANS:** A company is carrying out a survey that needs to be published using the desktop publication system, the employee’s data like (SSN, Department) need to be confidential without being made public

* 1. **Give an example of a type of publication in which data integrity is the most impor- tant requirement.**

**Ans :** Research and Developments based journals are a type of publication in which the data integrity is most important , as this impacts the both the results and views of the people going through the journals

* 1. **Give an example in which system availability is the most important requirement.**

**Ans:**  Twitter is an example of a system where system availability is considered of utmost importance. If there is any delay ,it makes a big news on the public and attracts negative reviews.

* **1.5**Consider the following general code for allowing access to a resource: DWORD dwRet = IsAccessAllowed(...); if (dwRet == ERROR\_ACCESS\_DENIED) { // Security check failed.   // Inform user that access is denied.
* } else {
* // Security check OK.
* }
  1. **Explain the security flaw in this program.**
  2. **Rewrite the code to avoid the flaw.**
* *Hint*: Consider the design principle of fail-safe defaults.  ?

Ans : a) According to the principle of fail-safe defaults ,access decisions should be based on permissions instead of exclusions. In the above code, it is checking if the above code has any error access denied condition only and informing the user about it, otherwise it says the check is ok and the access is given. This is a flawed approach as it is excluding users if any access denied conditions arises. The failure situation could go unnoticed for long time .

b) Instead it should be a permission based mechanism where task is performed only when the if condition or permission condition is true as shown below:

* DWORD dwRet = IsAccessAllowed(...);
* if (dwRet == NO\_ERROR) {
* // Security check passed.
* // Perform desired task
* } else {
* // Security check Failed.
* //Inform the user that the permission is denied
* }

3. Consider the block encryption algorithm TEA described in problem 2.4 in the textbook. In the description, ⊕ denotes bitwise exclusive OR (XOR), denotes addition modulo 232 , x y denotes circular left shift of value x by y bits, and x y denotes circular right shift of x by y bits.

(a) Suppose we are given this algorithm that consists only of two rounds and produces ciphertext C = (L2, R2). Express the ciphertext as a function of the input, i.e., the message and key blocks as well as the constants δi .

(b) Assume that the constants δi are publicly known. You don’t have the knowledge of the key, but can mount the chosen plaintext attack (i.e., request ciphertexts on messages of your choice). Given this ability, what information can you learn about the key using the 2-round version of TEA? Justify your answer.

(c) Would the answer described above change if the 4-round version of TEA is used instead? Justify your answer.

ANS: a) written in copy

b) written

c) written

4)

Read about AES-NI and research its use in programs. (a) Determine a way to use hardware accelerated AES in one programming language. Provide a segment of code to encrypt one block (16 bytes) of plaintext using AES hardware instructions such as aesenc, aesenclast, etc. Assume that the plaintext is initially stored in a binary buffer (array) and a 128-bit key is also stored in a binary buffer. Executing your code segment should result in a 16-byte cipher block. (b) Is hardware accelerated AES available in all programming languages? Explain. (c) List resources that were useful in working on this problem.

5B) encriptPlainText() for 1000 plainText took 0.022560 seconds to execute

That took 392 miliseconds in JAVA