**Principles of Cryptography**

**Class Activity: Introduction to Block Ciphers**

1. Describe in not more than 1 sentence what is meant by “Avalanche Effect” in block ciphers

**In cryptography, the avalanche effect is simply defined as a slight change in the input results in a significantly changed output.**

1. What is a weak key? Explain mathematically. Which algo is known to have weak keys?

**Weak keys are keys that are their own inverses. They include keys that have all 0s or all 1s or first half 1s and second half 0s and vice versa.**

**Mathematically: DESk1(m)=c => DESk2¯¯¯¯¯¯(c)=m**

* **This is a mathematical representation where the keys who inverses were other keys**

**DES is a known algorithm to have weak keys. Some possible weak keys in DES are keys that result in the same sub keys being used in multiple rounds.**

3. This question involves AES and DES encryption and decryption. Use the “openssl” utility that comes with the OpenSSL distribution to perform the following operations.

OpenSSL also runs on Windows platforms. You can download it from the following link

http://sourceforge.net/projects/gnuwin32/files/openssl/0.9.8h-1/openssl-0.9.8h-1-bin.zip/download

For help on how to run the commands you can refer to the following links

http://www.openssl.org/docs/apps/openssl.html#

http://www.openssl.org/docs/apps/enc.html

a) Download the encrypted file and the key file provided

Decrypt the file using 128 bit AES in ECB mode. Use the **“openssl enc”** command. It should result in a text file with a message in English. The output file should have “.txt” extension otherwise it will give you garbage. For decrypting the key file provided is sufficient and no other password is needed.

**openssl enc –aes-128-ecb -in ciphertextForSSL -out ciphertextForSSL.txt -d -kfile keyForSSL.txt**

**Text says:**

**This is to certify that you have now become a certified Security Professional after attending the information security course with Dr. Zahid. We hope you enjoyed studying this course and we wish you a successful career ahead.**

b) Use the “speed” option for the “openssl” command to compare the performance of AES in CBC mode using key lengths 128, 192, and 256 bits, DES in CBC mode, and triple DES (DES in EDE mode). The “speed options reports the bytes processed in a fixed amount of time. Report your results in bytes per second as reported by “openssl speed”. Rank the three in terms of performance.

In order of best performance to worst performance:

AES-128: #1



AES-192: #2



AES-256: #3



Triple DES: #4

