CMSC 414 (Shankar) **HW 1**

Note:

- This hw will count very little because all the problems are from old homeworks, but it's still worth doing carefully because it is relevant for exams.
- Some problems may not be graded.
- Due date and late policy on class web page.
- Submissions that are not neat and easily legible may get zero marks.

1. (text 3.5) Suppose the DES mangler function maps every 32-bit value to zero, regardless of the value of its input. What function would DES then compute?

2. (text 3.8) Why is a DES weak key its own inverse? (Hint: DES encryption and decryption are similar once the per-round keys are generated.)

3. (text 4.1) What pseudo-random block stream is generated by 64-bit OFB with a weak DES key.

4. (text 4.2) The pseudo-random stream of blocks generated by 64-bit OFB (i.e., K{IV}, K{K{IV}}, ...) must eventually repeat. Will K{IV} necessarily be the first block to be repeated. Explain.

5. (text 5.1) Would it be reasonable to compute an RSA signature on a long message m by signing m mod-n (i.e., using $(m \text{ mod-} n)^d \text{ mod-} n$ as the signature).

6. (text 5.6) Why do MD4, MD5, and SHA-1 require padding of messages that are already a multiple of 512-bits?

7. (text 6.8) Given your RSA signature on m_1 and m_2, how can one compute your signature on $m_1^j \cdot m_2^k$ for any positive integers j and k.

8. Using the efficient algorithm, compute 131^{25} mod-15.

9. Suppose a plaintext file of 5 MB is encrypted with a secret-key algorithm (e.g., DES, AES), and the resulting file is compressed with a lossless compression algorithm (e.g., zip), and the resulting file is 3 MB. What does this imply about the plaintext, about the encryption algorithm, and about the compression algorithm.