Homework 2
Introduction to Information Security (266-642)
Due Date: Oct 14 (Th), 2010

Note: You can talk to your classmates, instructor, and TA about the problems. However, unless stated otherwise, problems should be written up individually. University of Wisconsin rules for academic misconduct apply.
In the homework, "the Stallings book" refers to [2] and "the Handbook" refers to [1] (I have linked the Handbook to the class homepage. You can download it for free.)
In the homework Boneh-Shoup refers to the draft I mentioned in class. I have been handing out chapters from this draft.

Question 1 (OFB mode, 10 points): The following two questions are on the *output feedback mode* (*OFB*).
Part A: Prove that the encrypt and decrypt stages of the OFB mode work correctly, i.e., one obtains the plaintext after decryption. First, prove this for the first stage. After that, prove it in general for the i-th stage.

Part B: Explain the following quote from the book:

One advantage of the OFB method is that bit errors in transmission do not propagate.

Question 2 (Meet-in-the-Middle attack 10 points):
Suppose Triple DES is performed by choosing two keys K_1, K_2 and computing $E_{K_1}(E_{K_2}(E_{K_2}(m)))$ (note that the order of the keys has been modified from the usual two-key version of Triple DES). Show how to attack this modified version with a meet-in-the-middle attack.

Question 3 (10 points): Problem 3.2 from the Stallings book.

Question 4 (Block ciphers 25 points):
Part A: Problem 3.13 from the Stallings book.

Part B: Problem 3.15 from the Stallings book.

Question 5 (Number theory basics):
Part A (15 points): Solve the following system of equations using the algorithm given in class. Please show all the steps.

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 2 \pmod 7 \end{aligned}$$

Let z_1 and z_2 be two solutions to the system of equations given above. Argue that $z_1 \equiv z_2 \pmod{105}$.

Part B (15 points): A group of people are arranging themselves for a parade. If they line up three to a row, one person is left over. If they line up four to a row, two people are left over, and if they line up five to a row, three people are left over. What is the smallest number of people? What is the next smallest number? (*Hint:* Interpret this problem in terms of the Chinese remainder theorem (CRT)).
Part C (5 points): Divide 2^{10203} by 101. What is the remainder? (*Hint:* use Fermat's little theorem (FLT).).

Question 6 (DES 15 points) [Extra credit]: Find a key K such that $DES_K(\cdot) = DES_K^{-1}(\cdot)$. Such a key is sometimes called a *weak* key. How many weak keys can you find? Why do you think they are called weak?

Question 7 (RSA 20 points):
Part A: Prove that if Alice's exponent e is 3 and an adversary obtains Alice's secret exponent d, then the adersary can factor Alice's modulus n in time polynomial in the number of bits in n.
Part B: Prove that RSA is multiplicative in the following sense:

$$E_K(m_1)E_K(m_2) \equiv E_K(m_1m_2) \pmod{n}$$

Use this to show a chosen ciphertext attack on RSA.
Part C (10 points) [Extra credit]: Show that if an adversary had a procedure that could efficiently decrypt 1 percent of the encrypted messages from Z_n, then he could employ a probabilistic algorithm to decrypt every encrypted message with high probability.

References

[1] A.J. Menezes, P.C. Van Oorschot, and S.A. Vanstone. *Handbook of Applied Cryptography*. CRC press, 1997.

[2] William Stallings. *Cryptography and Network Security: Principles and Practice*. Prentice Hall, 2006.