

Homework #1

ISA 666 Internet Security Protocols Fall 2006

This homework is due on 09/19 by the end of class. This is an individual homework assignment to be done by each student individually. The submission of your homework is your acknowledgement of the honor code statement

"I have not taken any help on this assignment from anyone and not provided any help to anyone. The solution has been entirely worked out by me and represents my individual effort"

Please

- use a word processor (MS-Word, LaTeX, Framemaker, ...) for your solutions and submit your solutions (in pdf format) to the TA gmuisa666@gmail.com with "ISA 666 HW#1" as the subject in your email. Hard copy submission is not accepted.
- include your name and G-number at the beginning of your homework submission
- Your answer to the question is expected to be a technical solution.

1. Textbook Homework 2.2 (15 points)

2. Textbook Homework 2.5 (15 points)

3. Textbook Homework 3.4 (15 points)

4. Textbook Homework 3.5 (15 points)

5. The Mangler function takes a 32-bit R and XORs it with a 48-bit subkey. How is this possible? (10 points)

6. Decode this and explain how you did this : (20 points)

Mci vojs giqqsggtizzm sofbsr tizz aofyg tcf hvwg eisghwcb. Bck mci aigh kfwhs o rshowzsr sldzobohwcb ct hvs dfcsgg mci igr hc pfsoy hvwg qwdvsfshlh. Wt mci kfchs o gqfwdh, dzsogs gipawh wh og kszz. Hvs gqfwdh qob ps wb hvs dfcufoaawbu zobuious ct mcif qvcwqs. Hvs gqfwdh kwzz bch ps qvsqysr tcf dfcufoaawbu ghmzs, rsgwub cf sttwqwsbqm.

7. Let L_n , R_n , K_n denote 32-bit random numbers, and let $R_e(L_n, R_n, K_n) = (L_{n+1}, R_{n+1})$ represent the DES encryption round shown in the left diagram in Figure 3.6 in the textbook, which has included 2 functional mappings:

- $L_n \times R_n \times K_n \Rightarrow L_{n+1}$ (this means L_{n+1} is a function of L_n, R_n, K_n)
- $L_n \times R_n \times K_n \Rightarrow R_{n+1}$ (this means R_{n+1} is a function of L_n, R_n, K_n)

Prove that $R_e(R_{n+1}, L_{n+1}, K_n) = (R_n, L_n)$ (10 points)