Home ▶ My courses ▶ IS364 ▶ 4 March - 10 March ▶ Assignment 1

gation

Home

- My home

CVL-UDSM

My profile

My courses

IS364

Participants

General

25 February - 3 March

4 March - 10 March

Assignment 1

L/Unit 1: Encryption Basic Concepts Resource

Activity 2.1

11 March - 17 March

18 March - 24 March

25 March - 31 March

1 April - 7 April

8 April - 14 April

15 April - 21 April

Assignment 1

Assignment Problems

1. Create software that can encrypt and decrypt in Cipher Block Chaining mode using one of the following ciphers: affine modulo 256, Hill modulo 256, S-DES, DES. Test data for S-DES: using a binary initialization vector of 1010 1010, a binary plaintext of 0000 0001 0010 0011 encrypted with a binary key of 01111 11101 should give a binary plaintext of 1111 0100 0000 1011. Decryption should work correspondingly.
2. Create software that can encrypt and decrypt in 4-bit Cipher Feedback mode using one of the following ciphers: additive modulo 256, affine modulo 256, S-DES;

   or

   8-bit Cipher Feedback mode using one of the following ciphers: 2 x 2 Hill modulo 256. Test data for S-DES: using a binary initialization vector of 1010 1011, a binary plaintext of 0001 0010 0011 0100 encrypted with a binary key of 01111 11101 should give a binary plaintext of 1110 1100 1111 1010. Decryption should work correspondingly.
3. Create software that can encrypt and decrypt in 4-bit Output Feedback mode using one of the following ciphers: additive modulo 256, affine modulo 256, S-DES;

   or

   8-bit Output Feedback mode using one of the following ciphers: 2 x 2 Hill

22 April - 28 April

29 April - 5 May

6 May - 12 May

13 May - 19 May

20 May - 26 May

27 May - 2 June

3 June - 9 June

ings

Course administration

My profile settings

modulo 256.

4. Create software that can encrypt and decrypt in Counter mode using one of the following ciphers: affine modulo 256, Hill modulo 256, S-DES.Test data for S-DES: using a counter starting at 0000 0000, a binary plaintext of 0000 0001 0000 0010 0000 0100 encrypted with a binary key of 01111 11101 should give a binary plaintext of 0011 1000 0100 1111 0011 0010. Decryption should work correspondingly.

Submission status

Submission status	This assignment does not require you to submit anything online
Grading status	Not graded
Due date	Wednesday, 28 September 2011, 3:05 PM
Time remaining	The due date for this assignment has now passed