Navigation

Home

- My home

CVL-UDSM

My profile

My courses

IS364

Participants

General

25 February - 3 March

4 March - 10 March

11 March - 17 March

18 March - 24 March

25 March - 31 March

Activity 3.1

Assignment 2

L/Unit 1: Introduction to Number Theory Resource

L/Unit 2: Public Key Cryptosystems Resource

Activity 3.2

Assignment 2

Exercises

1.By Fermat's theorem, what is the multiplicative inverse of 2 in the field of integers mod 11?

2.With a public key encryption, suppose A wants to send a message to B. Let A_{PUB} and A_{PRIV} be A's public key and private key, respectively; similarly for B. Suppose C knows both public keys but neither private key. If A sends a message to B, what encryption should A use so that only B can decrypt the message? (This property is called secrecy.) Can A encrypt a message so that anyone receiving the message will be assured the message came only from A? (This property is called authenticity.) How or why not? Can A achieve both secrecy and authenticity for one message? How or why not?

3.Find keys d and e for the RSA cryptosystem where p = 7 and q = 11.

4.Is the DES an onto function; that is, is every 64-bit binary string the result of encrypting some string? Justify your answer.

5.Could the full 64 bits of a DES key be used, thereby giving it a strength of 2^{64} instead of 2^{56}? Justify your answer.

6.

1 April - 7 April
8 April - 14 April
15 April - 21 April
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

Settings

Course administration

My profile settings

a.Assume each S-box substitution takes 8 units of time (because of the eight 6-bit substitutions), each P-box permutation takes 4 units of time (counting 1 unit per byte), each expansion permutation takes 8 units of time (because of the eight 4-bit expansions and permutations) and each initial and final permutation takes 8 units. Compute the number of units of time for an entire 16-round cycle of the DES.

b.Now suppose DES were redesigned to work with a 112-bit key and a cycle on 128 bits of input, by increasing the number of S- and P-boxes. You do not have to define the details of this design. Using similar timing assumptions as in the first part of this question, compute the number of units of time for an entire 16-round cycle of 112-bit DES.

c.Perform a similar estimate for the timing of triple DES, using $E(k_1,D(k_2,E(k_1,m)))$.

7.Write a computer program that implements fast exponentiation (successive squaring) modulo n.

8. Reading: Security weaknesses of Public key cryptosystem.

Submission status

Submission status	This assignment does not require you to submit anything online
Grading status	Not graded
Due date	Wednesday, 21 September 2011, 3:45 PM
Time remaining	The due date for this assignment has now passed