International Institute of Information Technology Hyderabad

System and Network Security (CS5470)

Lab Assignment 2: Implementation of the Generalized Caesar Cipher with the help of Diffie-Hellman Key Exchange Protocol using Client-Server Model

Deadline: February 18, 2017 (23:55 P.M.)

Total Marks: 100 [Implementation (Coding + correct results): 75, Vice-voce: 25]

Note:- *It is strongly recommended that no student is allowed to copy programs from others. Hence, if there is any duplicate in the assignment, simply both the parties will be given zero marks without any compromise. Rest of assignments will not be evaluated further and assignment marks will not be considered towards final grading in the course. No assignment will be taken after deadline. Name your programs as roll_no_assign_2_client.c and roll_no_assign_2_server.c for the client and server, respectively. Upload your only client.c and server.c files in a zip file to course moodle portal. You are restricted to use only C programming language for implementation.*

Description of Problem

- **Part 1: Establishment of a shared session key $K_{A,B}$ between the client A and the server B:** For this part, you use the Diffie-Hellman key exchange protocol, which is described below:
  - *Global Public Elements*
    • q : a sufficiently large prime, such that it is intractable to compute the discrete logarithms in Z_q^*.
    • α : $\alpha < q$ and α a primitive root of q.
  - *User A Key Generation*
    • Select private X_A such that $X_A < q$
    • Calculate public Y_A such that $Y_A = \alpha^{X_A} \mod q$
    $A \rightarrow B : \{Y_A, q, \alpha\}$
    Here $A \rightarrow B : M$ denotes party A sends a message M to party B.
  - *User B Key Generation*
    • Select private X_B such that $X_B < q$
    • Calculate public Y_B such that $Y_B = \alpha^{X_B} \mod q$
    $B \rightarrow A : \{Y_B\}$

Table 1: Encoding used in Part 2.

A = 01	K = 11	U = 21	1 = 31
B = 02	L = 12	V = 22	2 = 32
C = 03	M = 13	W = 23	3 = 33
D = 04	N = 14	X = 24	4 = 34
E = 05	O = 15	Y = 25	5 = 35
F = 06	P = 16	Z = 26	6 = 36
G = 07	Q = 17	, = 27	7 = 37
H = 08	R = 18	. = 28	8 = 38
I = 09	S = 19	? = 29	9 = 39
J = 10	T = 20	0 = 30	! = 40

- *Generation of secret key by User A*
  • Compute the shared key with B as $K_{A,B} = (Y_B)^{X_A} \mod q$

- *Generation of secret key by User B*
  • Compute the shared key with A as $K_{B,A} = (Y_A)^{X_B} \mod q = K_{A,B}$

- **Part 2: Implementation of Generalized Caesar Cipher using the Established Key in Part 1.** Consider a set of alphabet of definition, which consists of the characters provided in Table 1. Also, we use the encoding technique given below. Assume that the upper case and lower case letters have the same digital alphabet. 00 indicates a space between words.

  - Alice (client A) encrypts the plaintext, say,
    The brown fox is quick!
    using a key $k = K_{A,B} \pmod{41}$, and sends the ciphertext to Bob (server B). Bob B will decrypt the ciphertext.
  - Bob (server B) encrypts the plaintext, say,
    Meet me after the toga party at 10 P.M. night at IIIT main gate.
    using a key $k = K_{A,B} \pmod{41}$, and sends the ciphertext to Alice (client A). A will decrypt the ciphertext.