RAMAIAH
UNIVERSITY
OF APPLIED SCIENCES

ASSIGNMENT

Course Code	CSC201A
Course Name	Discrete Mathematics - I
Programme	B.Tech
Department	CSE
Faculty	FET

Name of the Student	Satyajit Ghana
Reg. No	17ETCS002159
Semester/Year	03/2018
Course Leader/s	Ms Sahana

Declaration Sheet

Student Name	Satyajit Ghana		
Reg. No	17ETCS002159		
Programme	B.Tech	Semester/Year	03/2018
Course Code	CSC201A		
Course Title	Advanced Programming Concepts		
Course Date		to	
Course Leader	Ms Sahana		

Declaration

The assignment submitted herewith is a result of my own investigations and that I have conformed to the guidelines against plagiarism as laid out in the Student Handbook. All sections of the text and results, which have been obtained from other sources, are fully referenced. I understand that cheating and plagiarism constitute a breach of University regulations and will be dealt with accordingly.

Signature of the Student		Date	
Submission date stamp (by Examination & Assessment Section)			

Signature of the Course Leader and date	Signature of the Reviewer and date

List of Tables

Table No.	Title of the table	Pg.No.

List of Figures

Question No. 1

Solution to Question No. 1 Part A:

A 1. Deffie-Hellman Key Exchange and its applications:

Introduction:

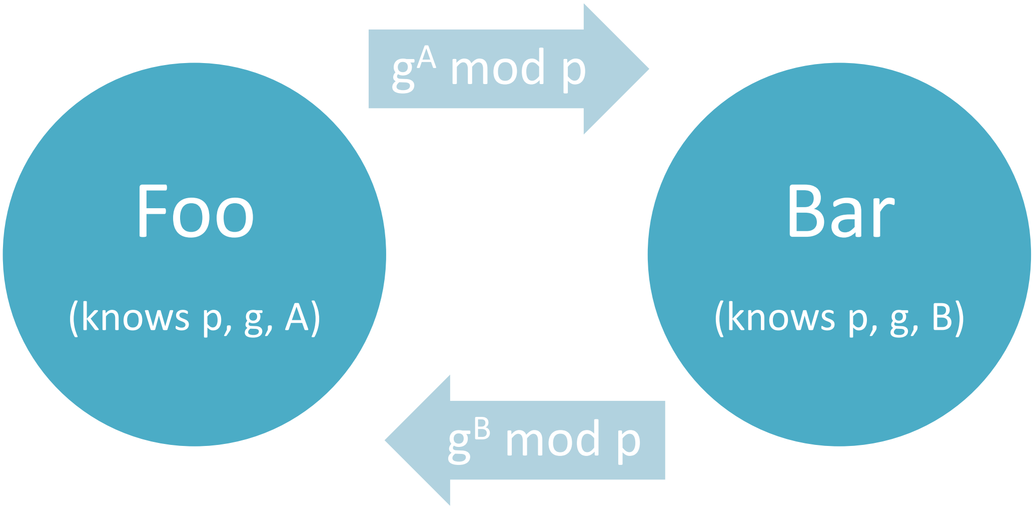
DH is a mathematical algorithm that permits two PCs to produce an indentical shared secret on both systems, despite the fact that those systems might never have communicated with one another. That shared secret can then be utilized to safely exchange a cryptographic encryption key. That key then encrypts traffic between the two systems.

Diffie-Hellman is not an encryption mechanism as we regularly consider them, in that we don't commonly utilize DH to encrypt data. Rather, it is a strategy for secure exchange of the keys that encrypt data. DH performs this protected exchange by making a "shared secret" (once in a while called a "Key Encryption Key" or KEK) between two devices. The shared secret then encrypts the symmetric key for secure transmittal. The symmetric key is some of the time called a "Traffic Encryption Key" (TEK) or "Data Encryption Dey" (DEK).

The procedure starts when every side of the correspondence generates a private key. Every side then produces a public key, which is a derivative of the private key. The two systems then exchange their public keys. Every side of the correspondence now has its own private key and the other system's public key

By running the mathematical operation against your own private key and the other side's public key, you produce a value. At the point when the far-off end runs the same operation against your public key and its own private key, that end also creates a value. The critical point is that the two qualities produced are identical. They are the "shared secret" that can encrypt data between systems.

Steps:



1. Foo and Bar agree on a prime number p and a base g.
2. Foo chooses a secret integer a, then sends Bar

$$A = g^a \ mod \ p$$

3. Bar chooses a secret integer b, then sends Foo

$$B = g^b \ mod \ p$$

4. Bar computes

$$K_1 = B^a \ mod \ p$$

5. Foo computes

$$K_2 = A^b \ mod \ p$$

6. Foo and Bar now share a secret i.e. both Bob and Alice can use this number as their key.

Applications:

a. Secure Sockets Layer (SSL)

SSL is all about encryption. SSL uses certificates, private/public key exchange pairs and Diffie-Hellman key agreements to provide privacy (key exchange), authentication and integrity with Message Authentication Code (MAC). This information is known as a cipher suite and exists within a Public Key Infrastructure (PKI). SSL is useful for business/financial traffic, e.g. credit card transactions. SSL ensures confidentiality (it prevents eavesdropping), authenticity (the sender is really who he says he is), and integrity (the message has not been changed en route). It is possible that a user might not know SSL is used in the course of communication but they are likely to notice some blockages.

b. Secure Shell (SSH)

SSH is a network security protocol very common for secure remote login on the Internet. The protocol proceeds in three stages. The first of these is the “Hello” phase, where the first identification is done. A list of supported algorithms is involved here after the first “Hi” message, and this list details the supported Diffie-Hellman key groups, among other things. The second stage sees the two parties agree upon a shared secret key x, which is done by an implementation of a Diffie-Hellman exchange. At the final stage, the shared secret key, session identifier and digest are used to generate the application keys.

c. IP Security (IPSec)

Like the previous protocols, IPSec uses D-H and asymmetric cryptography to establish identities, preferred algorithms, and a shared secret. Before IPSec can begin encrypting the data stream, some preliminary information exchange is necessary. This is accomplished with the Internet Key Exchange (IKE) protocol. IKE uses DH to produce a shared secret via the usual mechanisms, and then authenticate each other; after that, the secret key is used for encryption purposes. This shared secret key is never exchanged over the insecure channel

Question No. 2

Solution to Question No. 1 Part B:

B 1.1 Solution of the recurrence relations:
Given the recurrence relation,

$$s_n = a_1 s_{n-1} + a_2 s_{n-2} + a_3 s_{n-3} \qquad -(1)$$

Where s_n denotes the data transferred during the n^{th} hour of the operation.

Also, the values of s_n for $n = 0,1,2,3,4,5$ are $44, -3.87138, 16.4883, -12.9416, 9.9215, -12.3688$.

The value of a_1, a_2, a_3 are obtained by substituting $n = 3,4,5$ in (1) and then solving the system of linear equations.

$$a_1 s_2 + a_2 s_1 + a_3 s_0 = s_3$$
$$a_1 s_3 + a_2 s_2 + a_3 s_1 = s_4$$
$$a_1 s_4 + a_2 s_3 + a_3 s_2 = s_5$$

After substituting,

$$\begin{pmatrix} 16.4882 & -3.87138 & 44 \\ -12.9416 & 16.4883 & -3.87138 \\ 9.9215 & -12.9416 & 16.4883 \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} = \begin{pmatrix} -12.9416 \\ 9.9215 \\ -12.3688 \end{pmatrix}$$

$$\begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} = \begin{matrix} 0.28622 \\ 0.74758 \\ -0.35560 \end{matrix}$$

Substituting these values in (1)

$$s_n = 0.28622 s_{n-1} + 0.74758 s_{n-2} - 0.35560 s_{n-3}$$

The characteristic equation is,

$$r^3 - 0.28622 r^2 - 0.74758 r + 0.35560 = 0$$

Roots for this equation are,

$$\begin{pmatrix} r_1 \\ r_2 \\ r_3 \end{pmatrix} = \begin{matrix} -0.9210509 \\ 0.6053581 \\ 0.6019166 \end{matrix}$$

$$r = -0.9210509, 0.6053581, 0.6019166$$

Now, Solution for (1) is

$$s_n = b_1 r_1^n + b_2 r_2^n + b_3 r_3^n \quad -(2)$$

To find the values of b_1, b_2, b_3 we substitute $n = 0, 1, 2$ to obtain 3 equations in 3 variables,

$$s_0 = b_1 r_1^0 + b_2 r_2^0 + b_3 r_3^0$$
$$s_1 = b_1 r_1^1 + b_2 r_2^1 + b_3 r_3^1$$
$$s_2 = b_1 r_1^2 + b_2 r_2^2 + b_3 r_3^2$$

$$\begin{pmatrix} 1 & 1 & 1 \\ -0.92105 & 0.605358 & 0.601916 \\ 0.848334 & 0.366458 & 0.362303 \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} = \begin{pmatrix} 44 \\ -3.8713 \\ 16.4883 \end{pmatrix}$$

$$\begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} = \begin{matrix} 0.0159999 \times 10^3 \\ -0.73997918 \times 10^3 \\ 1.76797923 \times 10^3 \end{matrix}$$

Substituting values of r and b in (2)

$$s_n = 1767.979236 \times 0.6019165917^n - 1739.979186 \times 0.6053581886^n + 15.99994951 \times (-0.9210509025)^n$$

B 1.2 Verification of correctness of the solution:

B 1.3 Computation and plotting the amount of data transferred:
Plot when n can take every value from 0 to 50, and excluding the imaginary output.

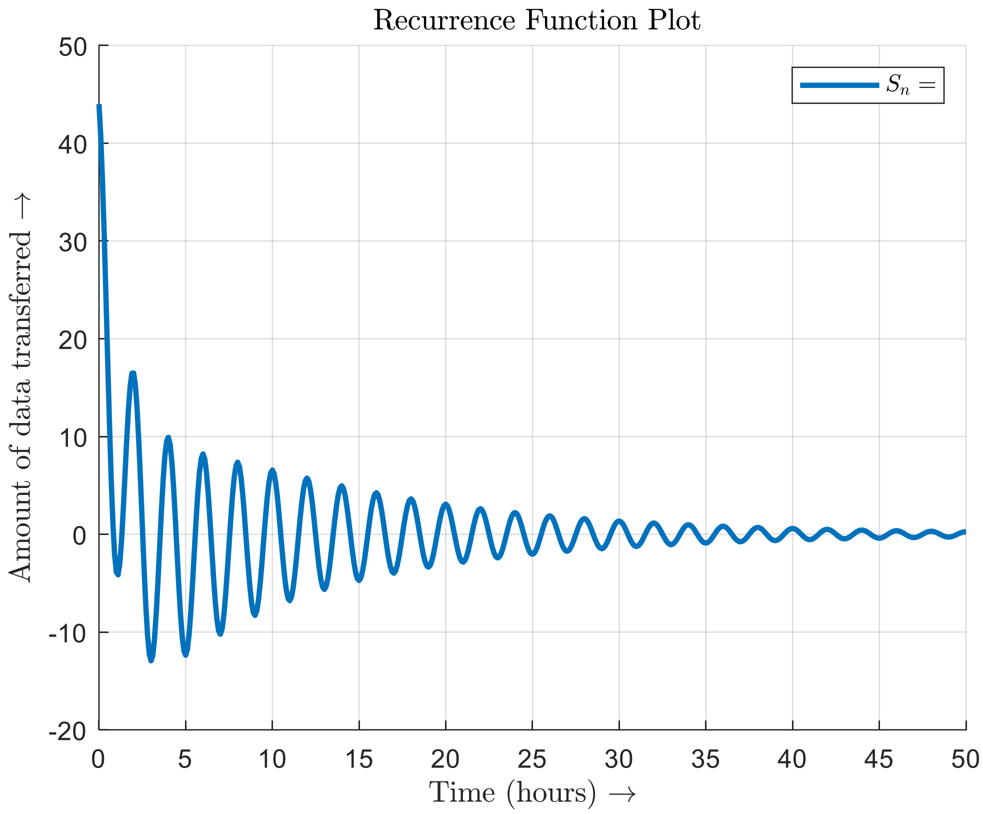


Figure B1.1: Recurrence Relation Plot

```
syms n;
sn = 1767.979236*0.6019165917^n - 1739.979186*0.6053581886^n + 15.99994951*(-
0.9210509025)^n;
x = 0:1:50;
y = subs(sn, x);
plot(x, y);
hold on;
grid on;
legend({'$S_n$'}, 'Interpreter', 'latex');
title("$ $ Recurrence Function Plot", 'Interpreter', 'latex');
xlabel("Time (hours) $\rightarrow$", 'Interpreter', 'latex');
ylabel("Amount of data transferred $\rightarrow$", 'Interpreter', 'latex');

disp('Amount of Data Transferred at the 50th Hour');
disp(vpa(subs(sn, 50), 30))
disp('Total Amount of Data Transferred from 0th to 50th Hour');
sum = 0;
for i=0:50
    sum = sum + subs(sn, i);
end
disp(vpa(sum, 30))
```

OUTPUT:

```
Amount of Data Transferred at the 50th Hour
0.261999357014522273940464172937

Amount of Data Transferred from 0 to 50th Hour
40.6737912516503434289496451 71
```

Plot when n can take only discrete values from 0 to 50

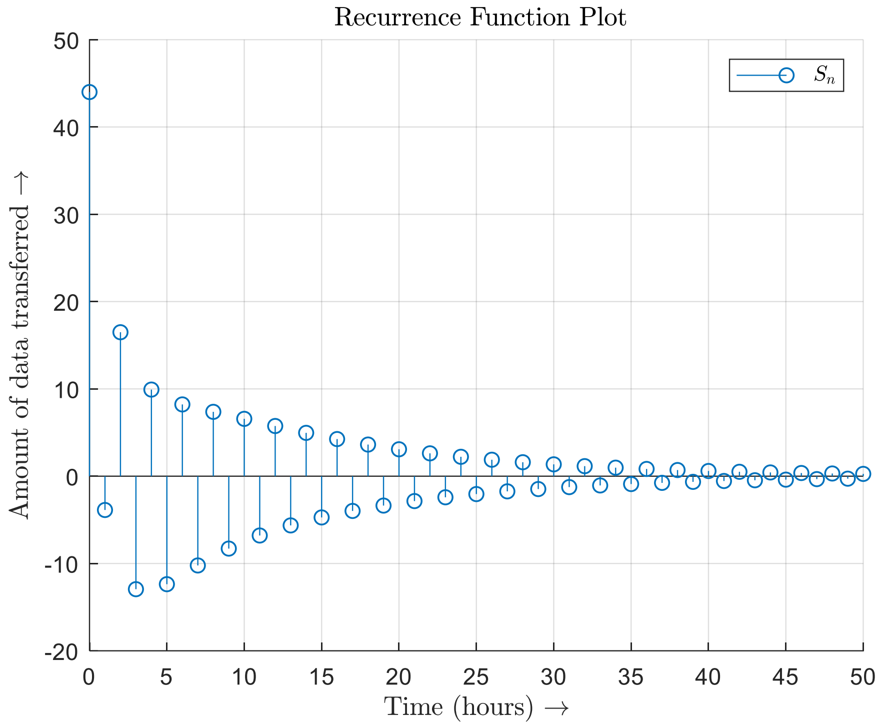


Figure B1.2 : Recurrence Relation Stem Plot for Discrete Values

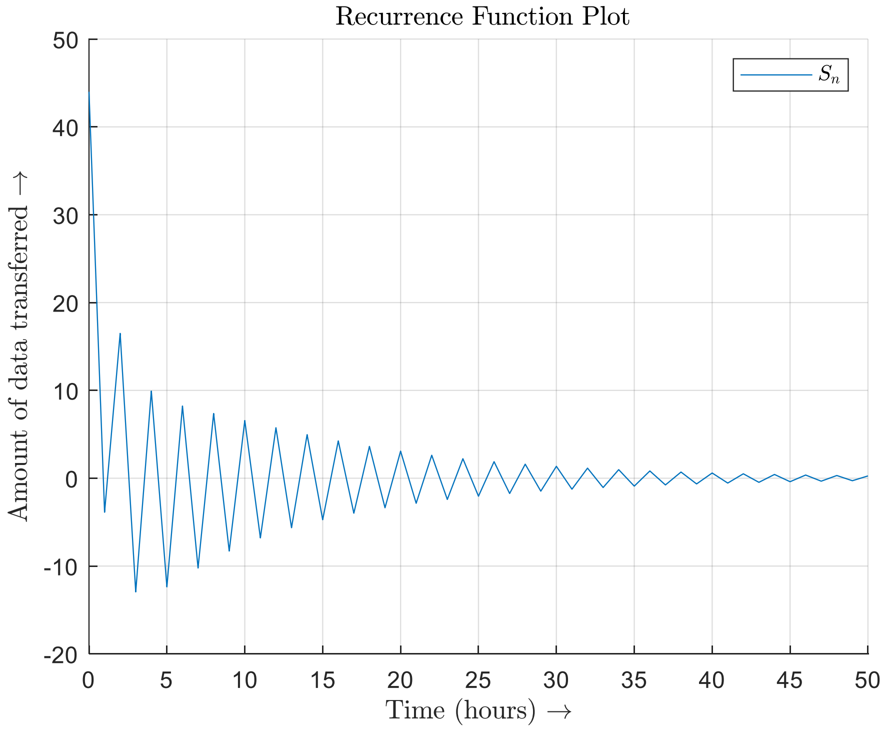


Figure B1.3 : Recurrence Relation Plot for Discrete Values

Question No. 3

Solution to Question No. 2 Part B:

B 2.1. Solution of the simultaneous equations:

Given the Linear-Congruence Relations

$$a_1 = 7; b_1 = 5; c_1 = 5; a_2 = 5; b_2 = 3; c_2 = 7; m = 7;$$

$$a_1x + b_1y \equiv c_1(mod\ m)$$

$$a_2x + b_2y \equiv c_2(mod\ m)$$

Or,

$$7x + 5y \equiv 5(mod\ 7) - (1)$$

$$5x + 3y \equiv 7(mod\ 7) - (2)$$

Method 1: Manually doing everything

The system of equations can be multiplied or divided by any x such that $\gcd(x, 7) = 1$

To eliminate the variable x, we want something like $7x - 6x$

We need to find $x \equiv 5^{-1}(mod\ 7)$, using Extended Euclid's Algorithm

$$7 = 5 \times 1 + 2 \qquad\qquad 7 - 5 \times 1 = 2$$

$$5 = 2 \times 2 + 1 \qquad\qquad 5 - 2 \times 2 = 1$$

$$5 - [7 - 5 \times 1] \times 2 = 1$$

$$5 \times 3 - 7 \times 2 = 1$$

Hence $5^{-1} \equiv 3(mod\ m)$

Multiplying (2) with 3

$$x + 2y \equiv 0(mod\ 7) - (3)$$

Multiplying this with 6

$$6x + 5y \equiv 0(mod\ 7) - (4)$$

$(1) - (3)$

$$x \equiv 5(mod\ 7)$$

Substituting this in (3)

And writing $x \equiv 5(mod\ 7)$ as $x = 7k + 5$, where $k \in \mathbb{Z}$

$$7k + 5 + 2y \equiv 0(mod\ 7)$$

$$2y \equiv -5\ (mod\ 7)$$

$$2y \equiv 2(mod\ 7)$$

$$y \equiv 1(mod\ 7)$$

Hence the answer is

$$x = 7k + 5$$

$$y = 7k + 1$$
$$\text{where } k \in \mathbb{Z}$$

<u>Method 2</u>: Using the Matrix Method, because the given values have gcd(vals, 7) = 1 and using only matrix operations such that gcd(operation, 7)=1

$$\begin{pmatrix} 7 & 5 \\ 5 & 3 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 5 \\ 7 \end{pmatrix} mod\ 7$$

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 5 \\ -6 \end{pmatrix} mod\ 7$$

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 5 \\ 1 \end{pmatrix}\ mod\ 7$$

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 7k + 5 \\ 7k + 1 \end{pmatrix}$$

Which is the required solution.

B 2.2 Determining the complete set of solutions:

We have,

$$x = 7k + 5$$
$$y = 7k + 1$$
$$\text{where } k \in \mathbb{Z}$$
$$\mathbb{Z} = \{.\ .\ . -3, -2, -1,0,1,2,3\ \ .\ .\ .\}$$

Substituting these values,

$$x = \ .\ .\ . -16, -9, -2,5,12,19,26\ .\ .\ .$$
$$y = \ .\ .\ . -20, -13, -6,1,8,15,22\ .\ .\ .$$

B 2.3 Verification of the set of solutions:

Verified using MATLAB

Bibliography

1. Diffie-Hellman:Key Exchange and Public Key Cryptosystems, *Sivanagaswathi Kallam*.
2. Diffie-Hellman and Its Application in Security Protocols (2012), *Maryam Ahmed, Baharan Sanjabi, Difo Aldiaz, Amirhossein Rezaei, Habeeb Omotunde*