

Implementation and Utilization of an Encryption Algorithm on M-commerce Background: Achieve Security

Prof. (Dr.) Jaydipkumar Hitendrabhai Trivedi

Received 28 February 2021; Accepted 13 March 2021

Abstract:- The Present Research work is suggesting an advance encryption algorithm. Propose algorithm is working on M-commerce background. Implementation and utilization of encryption algorithm is performing practically on M-commerce background. There are some input, output and process which suggest the text to be encrypted. The research work is based on purely experimental. It shows the importance of encryption algorithm for security purpose. The work is studying the existing encrypting algorithm with their respective background and observing security. The study shows the need of the encryption algorithm on various area of the computer science.

Key Words: M-commerce, Encryption Algorithm

I. INTRODUCTION

As we know, the implementation of programming is done on the basis of algorithm. Here, the algorithm is working on real e-commerce, m-commerce, and database background and achieving security. On M-commerce background, broadcasting agent and its receiving agent based implementation, utilization of algorithms have noted. Here, Webcasting is a identical type of broadcasting. "Broadcasting and Its Receiving Agent Based M-commerce Model", is the base model for the present model.^[1] For establishing security the work is suggesting encrypting and decrypting the text. The work is stating the depiction of restricted architecture of the particular types of broadcasting. Compressions of existing algorithm have observed.

II. ITERATURE REVIEWS

Trivedi J H, Darji J H, Patel H D, Trivedi P H, Designing And Prototyping Encryption Algorithms: Working As Secure Transaction of Broadcasting and Its Receiving Agent Based M-Commerce have achieved the security on the basis of encryption algorithm.^[3] The work had utilized encryption algorithm with single addition and subtraction of the text. But the present work is suggesting algorithm with different advancement. Trivedi J H, Pandya J G, Jani A N, Trivedi P H , Broadcasting And Its Receiving Agent Based M-Commerce Business Model, is instructing the base information for broadcasting agent based m-commerce transactions. But the present work is working on the same m-commerce background with different advancement with the different secure algorithm. Trivedi J H, Patel J M, Trivedi H J, Pipaliya K D, Applying Encrypting Algorithm Practically On M-Commerce Background: Observe Security and Crucial Performance, the work states the development of algorithm and observe the related security and a leveled performance of it. But the present work also implementing and utilizing the encryption algorithms with advancement and different advance algorithm with different result.

III. OBJECTIVES

To provide advancement in M-commerce background
To explore advance encryption algorithm for security purpose
To suggest a new algorithm for M-commerce base model and to study existing algorithm

IV. RESEARCH METHDOLOGY

The work is based on purely experimental. As Input, data have used for the algorithms to achieve result.

V. .HYPOTHESIS

An encryption algorithm is performing encrypting text, and decrypting text.
Encrypting and decrypting achieve security by hiding its real text.

VI. IMPLEMENTATION OF AN ENCRYPTION ALGORITHM

1. Study Existing Algorithms :

CASE ALGORITHM 1:

As per An Introduction to Database Systems by C.J Date, An Encryption Algorithms is as follows,

AS KINGFISHAR CATCH FIRE (Plain Text)

ELIOT (Encryption Key)

Step 1.

AS+ KINGFISHAR+CATCH FIRE

(Write the plain text into a state of length equal to that of that of encryption key)

Step 2,

“+” (Blank is indicating)

0119001109 1407060919 0805181900 0301200308 0006091805

(Convert the plain text by inter in the range 00-26 using blank =00, A=01, b=02,j=10)

Step 3

0512091520

(Use the step second for converting encryption key into integer form.)

Step 4

0119001109 1407060919 0805181900 0301200308 0006091805

0512091520 0512091520 0512091520 0512091520 0512091520

(For all block convert character by the sum modulo 27 of its integer encoding and the integer encoding of character of the encryption key)

FDIZB SSOXL MQ+GT HMBRA ERRFY

(Convert all integers encoding the result of step 4 by its character equivalent)^[2]

CASE ALGORITHM 2:

As per the research work, Trivedi J H, Darji J H, Patel H D, Trivedi P H, Designing And Prototyping Encryption Algorithms: Working As Secure Transaction of Broadcasting and Its Receiving Agent Based M-Commerce have achieved the security on the basis of encryption algorithm. The Encryption Algorithm is as follows,

Step 1:

TRIVEDI-JAYDIPKUMAR-H

(Plain text as message obtained)

(Converts the character to its related alphabetical digit like A=01, B=02, C=03, D=04)

(In the plain text blanks seems as “-“)

(Indicates Space as 00)

Step 2:

20180922050409001001 25040916112113011800 08

(Decide the digital block of the string as per the length of user name of e-mail address's digit)

Step 3:

mrjlecturer (obtained from mrjlecturer@yahoo.com)

(The encryption key formed on the basis of user name of e-mail address taken form

e-mail message for business Transaction is taking user name of e-mail address Only without “@” and rest of the address like yahoo mail.com)

1318101205032021180518 (Encryption key got from username)

(Converts the character to its related alphabetical Digit like A=01, B=02, C=03, D=04)

Step 4:

2018092205040900100125 04091611211301180008

1318101205032021180518 13181012050320211805

3336193410072921280643 17272623261621391813

(Sum the digital block of the string with Encryption key)

Step 5:

CCCFAICDA00GBIBABH0FDC AGBGBFBCBFAFBACIAHAC

(The obtained result of the sum from step 4 converted the digital string into alphabetical

String like 3=C, 9=I, and keep Zero “0” remain Same for further task, It means “0” is

Encrypted as “0” only.)

Encrypted Message:

CCCFAICDA00GBIBABH0FDC AGBGBFBCBFAFBACIAHAC

Step 6:

CCCFAICDA00GBIBABH0FDC AGBGBFBCBFAFBACIAHAC

3336193410072921280643 1727262 3261621391 813

(Converted the alphabetical string into digital String like C=3, I=9, and keep Zero “0”

Remain Same for further task, It means “0” is encrypted as “0” only.)

Step 7:

3336193410072921280643 17272623261621391813

1318101205032021180518 13181012050320211805
2018092205040900100125 04091611211301180008
(Subtracted the digital block of the string with Encryption key)

Step 8:
2018092205040900100125 040916112113 01180008
T R I V E D I - J A Y D I P K U M A R - H
(Obtained alphabetical string on the basis of result acquired from subtraction)^[3]

2. Need for Algorithm:

- From Case Algorithm 1, It is initial so it is easy to bypass the system, any un authorized person can use.
- From Case Algorithm 2, It is advance at a selected level for a time. But It needs advancement for future.

3. Implementation of Algorithms:

Encrypting and decrypting the text is using for establishing security in database. On internet, Update version of encryption and decryption is desirable. Even in m-commerce sites are using advance version of encryption and decryption.

First Cycle:

Step 1. Vishvam P Trivedi (As Plain Text)

Step 2. “_” (Under Score is using for blank Space)

Step 3, Text Convert As Per Below Style as Alfa Numeric.

(A will be 01, B will 02, C will be 03, and so on till Z. Z will 20. Then Numeric value will be taken 27,28,29,30 and its value will be same 27,28,29,30)

Example: Alphanumeric

A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z, 27,28,29,30,31,32,33,

01,02,03,04,05,06,07,08,09,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26, 27,28,29,30,31,32,33

Now, Step 1.is written as Vishvam_P_Trivedi will be Written as 22101908221300160020180922050409

Step 4. Convert the text in alphanumeric place number digit, and add 01.

(V has alphanumeric place number digit 22, and now adding 01 so It will be 23,

I has alphanumeric place number digit 10, and now adding 01 so It will be 11,

S has alphanumeric place number digit 19, and now adding 01 so It will be 20,

H has alphanumeric place number digit 08, and now adding 01 so It will be 09,

V has alphanumeric place number digit 22, and now adding 01 so It will be 23,

M has alphanumeric place number digit 13, and now adding 01 so It will be 14,

_ will be taken 00 and now adding 01 so It will be 01,

P has alphanumeric place number digit 16, and now adding 01 so It will be 17,

_ will be taken 00 and now adding 01 so It will be 01

T has alphanumeric place number digit 20, and now adding 01 so It will be 21,

R has alphanumeric place number digit 18, and now adding 01 so It will be 19,

I has alphanumeric place number digit 09, and now adding 01 so It will be 10,

V has alphanumeric place number digit 22, and now adding 01 so It will be 23,

E has alphanumeric place number digit 05, and now adding 01 so It will be 06,

D has alphanumeric place number digit 04, and now adding 01 so It will be 05,

I has alphanumeric place number digit 09, and now adding 01 so It will be 10.)

After addition our text will be like 23112009231401170121191023060510

Step 5. Take Encryption key, Here our Cell Phone Number Will Be Our Encryption key.

(Cell Phone Number is 9974706718 so we are using as 09 09 07 04 07 00 06 07 01 08)

Step 6. Divide the full text Digit as per encryption key digit and making block.

Our Text	23112009231401170121	191023060510
Cell Phone Number	09090704070006070108	090907040700

Step 7. Now perform addition of both the number

	23112009231401170121	191023060510
	09090704070006070108	090907040700
Addition Will be	32202713301407240229	281930101210

Step 8. Convert the result in Alphanumeric form for our main text which is Encryption.

32T27M30NGXB29 28S30JLJ

Step 9. Now obtained result convert in digital form and subtract with encryption key as cell phone number.

	32202713301407240229	281930101210
	09090704070006070108	090907040700
Subtraction will be	23112009231401170121	191023060510

Step 10. Now Subtracting 01 from obtained the result.

22101908221300160020180922050409

(Alphanumeric Convert As Per Below Style as Text.

A will be 01, B will 02, C will be 03, and so on till Z. Z will 20. Then Numeric value will be taken 27,28,29,30 and its value will be same 27,28,29,30)

Example: Alphanumeric to Text.

01,02,03,04,05,06,07,08,09,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26, 27,28,29,30,31,32,33

A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z, 27,28,29,30,31,32,33,)

Step 11. Now, result is written as 22101908221300160020180922050409 will be written as

Main text as step 1. Vishvam_P_Trivedi

Step 11. Result: Vishvam_P_Trivedi

Second Cycle:

Here, we are performing the same steps from Step 1 to Step 11.

- Input Plain Text:- Harakh_J_Trivedi is converted in alphanumeric using encryption

08011801110800110020180922050409

- Cell Phone Number As Encryption key:- 9426370114 converted in alphanumeric

09040206030700010104

- Text converted in alphanumeric form and divided in block as per Encryption Key

RFUHOPALBY 28NYLHQ

- Output Plain Text:- Harakh_J_Trivedi

Background of the Transaction:

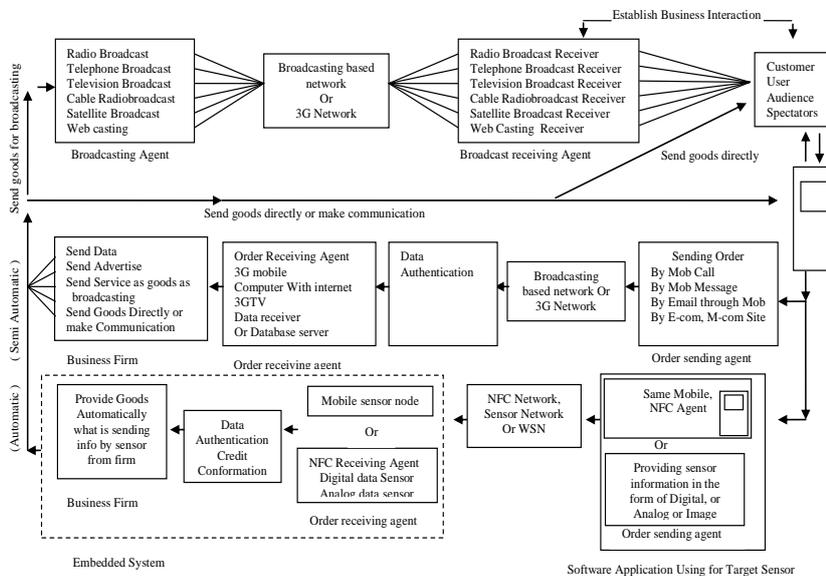


Figure 1: Architecture of the Broadcasting And It's Receiving Agents Based M-commerce Model

Present architecture instructs m-commerce transactions are perform automatically and semi automatically by customer using Broadcasting Agent and Its receiving Agents.^[2] Encryption is performing at the Embedded system. Here, there is a need of security for data. Data can be stored in encrypted form in database. So it will not be available simply for a stranger. A website or mobile phone app have capacity to manipulate data. But a person have access level.

VII. DATA AND ANALYSIS

Data At first Cycle:

- Input Plain Text :- Vishvam_P_Trivedi is converted in alphanumeric using encryption

22101908221300160020180922050409

- Cell Phone Number As Encryption key:- 9974706718 converted in alphanumeric

09090704070006070108

- Text converted in alphanumeric form and divided in block as per Encryption Key 32T27M30NGXB29

28S30JLJ

- Out Put Text:- Vishvam_P_Trivedi

Data At Second Cycle:

- Input Plain Text:- Harakh_J_Trivedi is converted in alphanumeric using encryption
08011801110800110020180922050409
- Cell Phone Number As Encryption key:- 9426370114 converted in alphanumeric
09040206030700010104
- Text converted in alphanumeric form and divided in block as per Encryption Key
RFUHOPALBY 28NYLHQ
- Output Plain Text:- Harakh_J_Trivedi

VIII. RESULT:

- From First Cycle Encrypted Text Is:- 32T27M30NGXB29 28S30JLJ
- From Second Cycle Encrypted Text Is:- RFUHOPALBY 28NYLHQ

IX. CONCLUSION

The work has utilized Encryption algorithm and obtained a text which is secure. Any stranger cannot understand this text. The work has suggested M-commerce background for its performance. The work has used “Broadcasting and Its Receiving Agent Based M-commerce Model” as base model. The work has used architecture of this model.

REFERENCE

- [1]. Trivedi J H, Pandya J G, Jani A N, Trivedi P H , “Broadcasting And Its Receiving Agent Based M-Commerce Business Model”, Research In Management, Research Journal Published by H N G University, Patan Vol.1
- [2]. An Introduction to Database Systems by C.J Date
- [3]. Trivedi J H, Darji J H, Patel H D, Trivedi P H, “Designing And Prototyping Encryption Algorithms: Working As Secure Transaction of Broadcasting and Its Receiving Agent Based M-Commerce have achieved the security on the basis of encryption algorithm.”,IOSR Journal of Engineering ISSN (e): 2250-3021, p-ISSN: 2278-8719 Vol. 3, Issue 8 (August. 2013), ||V3|| PP 25-33
- [4]. Trivedi Jaydipkumar H, Dr. Pandya J G, Patel Jignasha B, Mithapare Anita K, “M- Commerce Driving Factor and Transaction Variables: Aspects That Constructs The M-commerce Model”, IOSR Journal of Engineering ISSN (e): 2250-3021,ISSN (p): 2278-8719 (Vol.1,Issue 2,pp.135-141).
- [5]. Trivedi J. H, Trivedi P. H, Thakkar S. T, Makwana M.N, “Automatic and Semi Automatic Transaction of Broadcasting and It’s Receiving Agent Based M-commerce Business Model”, IOSR Journal of Engineering ISSN (e): 2250-3021, ISSN (p): 2278-8719 Vol. 3,Issue 2 (Feb-2013), PP 42-53.
- [6]. D Xiaojun,I Junchi, H Sho, “Unique features of mobile Commerce”, TITECH, 152-8552, Japan.

Prof. (Dr.) Jaydipkumar Hitendrabhai Trivedi. “Implementation and Utilization of an Encryption Algorithm on M-commerce Background: Achieve Security.” *IOSR Journal of Engineering (IOSRJEN)*, 11(02), 2021, pp. 46-50.