Secured Symmetric Key Encryption Algorithm with Modified Rail Fence Technique

Anjali Agrawal[1], Gaurav Kumar Ameta[2], Akhilesh Deep Arya[3]

[1, 2] *Department of Computer Science and Engineering, Pacific Institute of Technology, Udaipur, Rajasthan, India*

[3] *Department of Computer Science and Engineering, Geetanjali Institute of Technical Studies, Udaipur, Rajasthan, India*

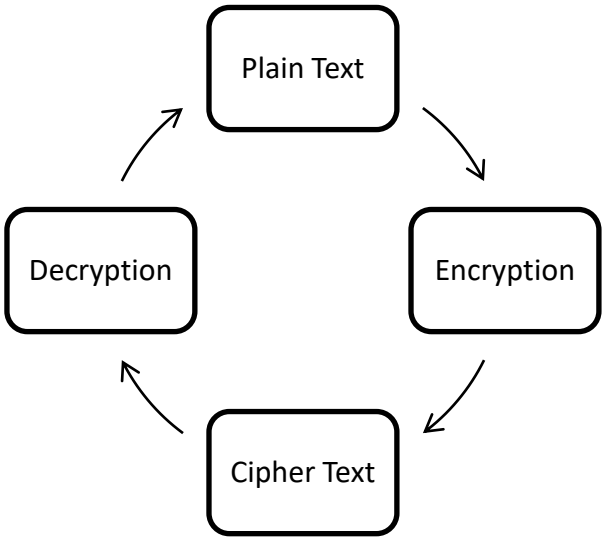
Abstract:- **With the exposure to World Wide Web and emergence of social networks, ecommerce applications and many organizations all over the world produces enormous amount of data. Security of data is the main aspect in today's computerized world it is important to provide the necessary protection to the information being exchanged over the internet from the intruders. As number of internet users is increasing day by day the number of cyber attacks is also increasing. It is a critical issue to provide security to our computers and networks. Cryptography provides security to data and information on network. In this paper we developed a technique which will help to enhance the data security.**

Keywords: **Cipher, Cryptography, Encryption Model, Symmetric key cryptography, Rail Fence Technique, Modified Rail Fence**

I. INTRODUCTION

Cryptography is a technique which provides security to the data or information being exchanged over the network. It converts the data or information, which is in human readable format, into unreadable format.

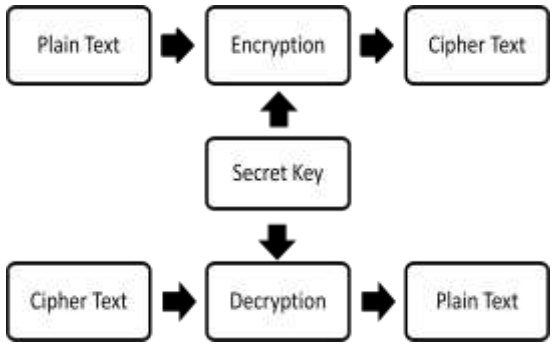
The original data in readable format is called plain text and the generated unreadable format is called cipher text. Encryption is transformation of plain text into cipher text and decryption is transformation of cipher text into plain text.



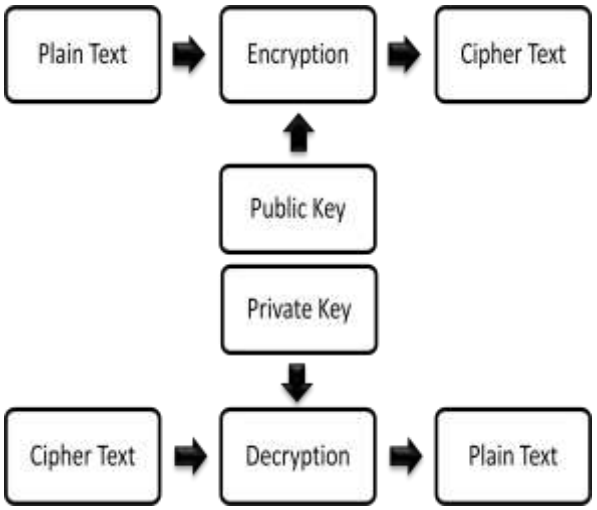
Cryptography is closely related to the development of algorithms for encryption and decryption, where as the term cryptanalysis is used for analysing and breaking the encrypted text. Cryptology is the study of both cryptography and cryptanalysis.

Key plays the major role in the process of encryption and decryption. Cryptography is categorized into two categories according to the number of keys used for encryption/decryption:

Symmetric Key Cryptography: This is also known as single key cryptography. This process uses a single key. The receiver and Sender have to agree upon a single secret key. Using this key the Plain text is transformed into cipher text. This cipher text is unintelligible data. For decryption the receiver uses the same key to generate the plain text. Only the sender and the receiver can decrypt the encrypted text, as only those two know about the key. This is also called private key cryptography.



Asymmetric Key Cryptography: Asymmetric key cryptography or public key cryptography uses two different keys for encryption and decryption. The two keys are: public key and private key. The public key is used for encryption. This key can be known to public. The private key is used for decryption, which is only known to the end user. Cipher Text generated with a public key can only be converted into plain text by using the corresponding private key. No key other then private key can decrypt the message, not even the public key used for encryption.



II. LITERATURE REVIEW

Arya A. et al. [1] developed a substitution based encryption model for cloud data storage which uses a ternary vector and random matrix as a key. The sequence for encryption is generated by multiplying these both and then applying the sign function. This algorithm uses a single key for both encryption and decryption so this key is securely shared between sender and receiver. The new encryption algorithm is based on the concept of Poly alphabetic cipher [10] which is an improved version of the mono alphabet [12].

They generated a 2 key based substitution encryption model in which 2 sequences are used for encryption. For the generation of second key inverse of random matrix is used. The second sequence is generated by multiplying it with ternary vector then applying sign function. First sequence is applied on plain text to generate cipher text then second key is applied on this cipher text to generate second cipher text, which is more secure. Analysis of this model is shown by calculating avalanche effect.

N Aarti, S Ajit and M Swati [8] combined the Caesar cipher and Rail fence technique with stack method for making the communication more secure. Caesar cipher is the simplest substitution method. It is also the weakest cipher. It can be easily detected. To overcome this problem N Aarti has merged Caesar cipher with transposition techniques. The transposition techniques they have used is rail fencing. For further complexity stacks are used which makes the detection of both the techniques difficult. This is a combination of transposition and substitution hence it provides better security for the text.

T S Ruprah [5] has proposed a new algorithm for encryption in which he has combined different symmetric algorithm in one with little change. In this encryption algorithm substitution techniques are combine with transposition techniques which makes it more secure and strong.

G Ritwik et al. [2] proposed a solution that uses cryptography to ensure confidentiality and integrity of involved data. It uses Rail Fence Technique (transposition technique) in combination with original Data Encryption Standard for speeding up the processing time and make it more complex and efficient

III. PRESENT WORK

We propose an algorithm which integrates substitution method and transposition method for encryption. Substitution method uses a ternary vector and a random matrix to generate first key for encryption and transposition technique uses modified Rail Fence technique [4] to generate the second key for encryption.

IV. DESIGN OF ALGORITHM

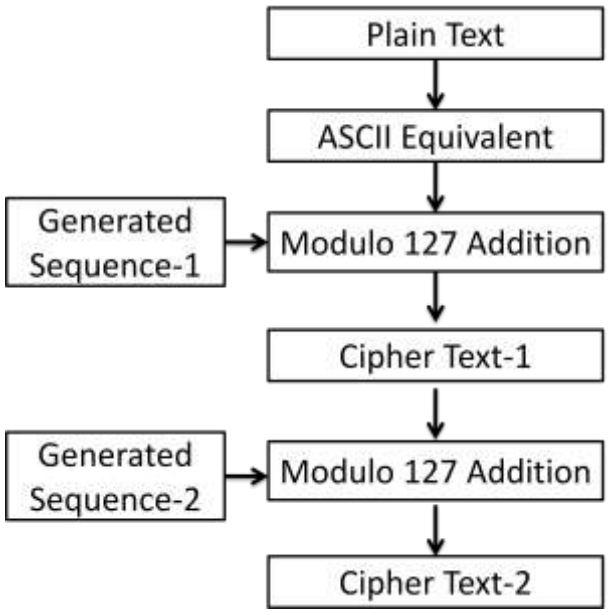
4.1 Adoptability of some mathematical functions in Cryptography

Sign Function [17]: This function is when applied on values of matrix, converts all the positive values to 1, negative values to -1 and zero with 0. The advantage of using this function in cryptography is it cannot be a reversible process, i.e., it is impossible to get back the original matrix by applying the process in reverse order.

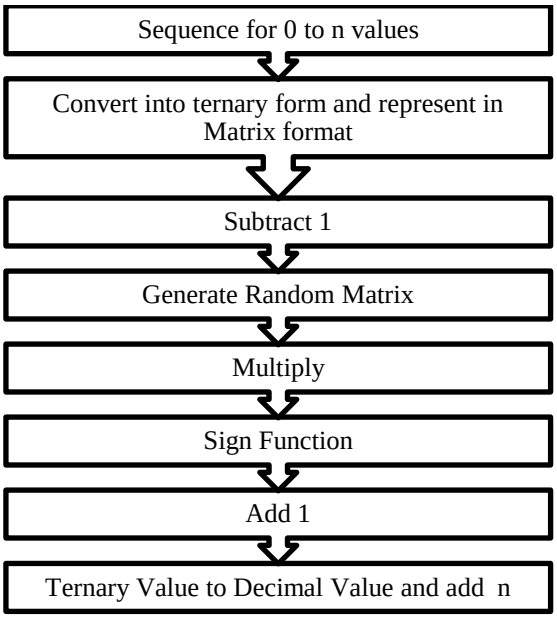
Modular Arithmetic [16]: One more function that is widely used in cryptography is modular arithmetic of a number with a base value. It will generate the remainder of a number with respect to the base value. This function is mostly used in public key cryptography.

4.2 Design Process

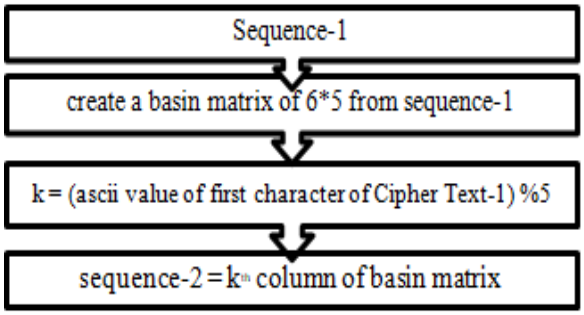
1. *Encryption*



Algorithm for generating the sequence-1



Algorithm for generating the sequence-2



Example:

Step1: Consider the sequence for n= 0 to 26 values.

Step2: Convert the sequence to ternary form of a 3 digit number.

i.e.

0 ------ 000

1 ------ 001

2 ------ 002

. .

. .

. .

26 ------ 222

Step3: Represent above ternary form in 27x3 matrix.

R =

0	0	0
0	0	1
0	0	2
0	1	0
0	1	1
0	1	2
0	2	0
0	2	1
0	2	2
1	0	0
1	0	1
1	0	2
1	1	0
1	1	1
1	1	2
1	2	0
1	2	1
1	2	2
2	0	0
2	0	1
2	0	2
2	1	0
2	1	1
2	1	2
2	2	0
2	2	1
2	2	2

Step 4: Subtract 1 from each element of the above matrix and the resultant matrix R is

R =

-1	-1	-1
-1	-1	0
-1	-1	1
-1	0	-1
-1	0	0
-1	0	1
-1	1	-1
-1	1	0
-1	1	1
0	-1	-1
0	-1	0
0	-1	1
0	0	-1
0	0	0
0	0	1
0	1	-1
0	1	0
0	1	1
1	-1	-1
1	-1	0
1	-1	1
1	0	-1
1	0	0
1	0	1
1	1	-1
1	1	0
1	1	1

Step 5: Consider a random matrix

$$A = \begin{bmatrix} -2 & 3 & 1 \\ 3 & -3 & 3 \\ 4 & -2 & -3 \end{bmatrix}$$

Step 6: R = R x A

R =

-5	-10	-32
-1	0	-1
3	10	30
-2	-4	-11
2	6	20
6	16	51
1	2	10
5	12	41
9	22	72
-7	-16	52
-3	-6	-21
1	4	10
-4	-10	-31
0	0	0
4	10	31
-1	-4	-10
3	6	21
7	16	52
-9	-22	-72
-5	-12	-41
-1	-2	-10
-6	-16	-51
-2	-6	-20
2	4	11
-3	-10	-30
1	0	1
5	10	32

Step 7: Convert all positive values to 1, negative values to -1 and zero to 0 of the resulting matrix in step 6.

R =

-1	-1	-1
-1	0	-1
1	1	1
-1	-1	-1
1	1	1
1	1	1
1	1	1
1	1	1
1	1	1
-1	-1	1
-1	-1	-1
1	1	1
-1	-1	-1
0	0	0
1	1	1
-1	-1	-1
1	1	1
1	1	1
-1	-1	-1
-1	-1	-1
-1	-1	-1
-1	-1	-1
-1	-1	-1
1	1	1
-1	-1	-1
1	0	1
1	1	1

Step 8: Add 1 to each element of matrix R.

R =

0	0	0
0	1	0
2	2	2
0	0	0
2	2	2
2	2	2
2	2	2
2	2	2
2	2	2
0	0	2
0	0	0
2	2	2
0	0	0
1	1	1
2	2	2
0	0	0
2	2	2
2	2	2
0	0	0
0	0	0
0	0	0
0	0	0
0	0	0
2	2	2
0	0	0
2	1	2
2	2	2

Step 9: Convert each row of the matrix R to decimal form to generate sequence, i.e., R[3] : 2 2 2 will form
$(2 * 3^2 + 2\%10) + (2 * 3^1 + 2\%10) + (2 * 3^0 + 2\%10) = 32$
Sequence-1 is

0	6	32	9	38	41	44	47	50	27
0	29	6	22	38	15	44	47	24	27
0	3	6	35	12	38	44			

Step 10: Now we will encrypt the given Plain Text into Cipher Text-1 using sequence-1 as Key.
Given Plain Text: 9876543

Plain Text	9	8	7	6	5	4	3
ASCII equivalent	57	56	55	54	53	52	51
Key	0	6	32	9	38	41	44
Add	57	62	87	63	91	93	95
Mod 127	57	62	87	63	91	93	95
Cipher text	9	>	W	?	[	]	_

Step 11: For sequence-2 we will create a basin matrix [3] with generated sequence-1. We will arrange sequence-1 in a 6*5 matrix. So our basin matrix is:

0	6	32	9	38
41	44	47	50	27
0	29	6	22	38
15	44	47	24	27
0	3	6	35	12
38	44	0	0	0

Step 12: Calculate k = (ASCII value of first character of Cipher Text -1)%5
k = 57%5 = 2

Step 13: sequence-2 is k^{th} column of our basin matrix.

0	6	**32**	9	38
41	44	**47**	50	27
0	29	**6**	22	38
15	44	**47**	24	27
0	3	**6**	35	12
38	44			

Step 14: Now we encrypt Cipher Text-1 into Cipher Text-2

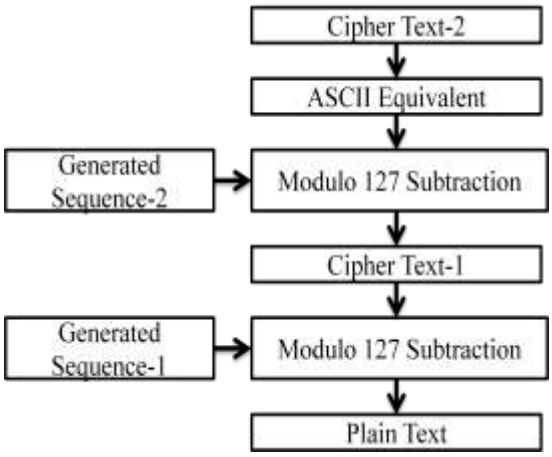
Cipher text-1	**9**	**>**	**W**	**?**	**[**	**]**	**_**
ASCII	**57**	**62**	**87**	**63**	**91**	**93**	**95**
Key	**32**	**47**	**6**	**47**	**6**	**32**	**47**
Add	**89**	**109**	**93**	**110**	**97**	**125**	**142**
Mod 127	**89**	**109**	**93**	**110**	**97**	**125**	**15**
Cipher Text-2	**Y**	**m**	**]**	**n**	**A**	**}**	

1. Encryption:

Plain Text	**9**	**8**	**7**	**6**	**5**	**4**	**3**
ASCII equivalent	**57**	**56**	**55**	**54**	**53**	**52**	**51**
Key	**0**	**6**	**32**	**9**	**38**	**41**	**44**
Add	**57**	**62**	**87**	**63**	**91**	**93**	**95**
Mod 127	**57**	**62**	**87**	**63**	**91**	**93**	**95**
Cipher text-1	**9**	**>**	**W**	**?**	**[**	**]**	**_**
ASCII equivalent	**57**	**62**	**87**	**63**	**91**	**93**	**95**

Key	**32**	**47**	**6**	**47**	**6**	**32**	**47**
Add	**89**	**109**	**93**	**110**	**97**	**125**	**142**
Mod 127	**89**	**109**	**93**	**110**	**97**	**125**	**15**
Cipher Text-2	**Y**	**M**	**]**	**n**	**A**	**}**	

2. Decryption



Cipher Text-2	**Y**	**m**	**]**	**n**	**a**	**}**	
ASCII equivalent	**89**	**109**	**93**	**110**	**97**	**125**	**15**
Key-2	**32**	**47**	**6**	**47**	**6**	**32**	**47**
Subtract	**57**	**62**	**87**	**63**	**91**	**93**	**-32**
Add 127 if negative	**57**	**62**	**87**	**63**	**91**	**93**	**95**
Cipher text-1	**9**	**>**	**W**	**?**	**[**	**]**	**_**
ASCII equivalent	**57**	**62**	**87**	**63**	**91**	**93**	**95**
Key-1	**0**	**6**	**32**	**9**	**38**	**41**	**44**
Subtract	**57**	**56**	**55**	**54**	**53**	**52**	**51**
Add 127 if negative	**57**	**56**	**55**	**54**	**53**	**52**	**51**
Plain Text	**9**	**8**	**7**	**6**	**5**	**4**	**3**

Analysis of the Proposed Models

Avalanche effect [11], is a desirable effect in cryptography. It means that the output have a very big change if we slightly change the input. A small change in the key or the plain text will lead to significant change in the cipher text.

Higher the Avalanche effect better is the algorithm. Strict avalanche criteria, transform approximately half of the plain text bits in to the output.

Avalanche Effect can be calculated using the formula

$$\text{Avalanche Effect} = \frac{\text{No .of flipped bits in the ciphered text}}{\text{No .of bits in the ciphered text}} \text{ X } 100$$

Plain Text : 9 8 7 6 5 4

Random Matrix A= $\begin{bmatrix} -2 & 3 & 1 \\ 3 & -3 & 3 \\ 4 & -2 & -3 \end{bmatrix}$

Using this Random Matrix Generated First Key is "0 6 32 9 38 41"

And second key is "32 47 6 47 6 32"

Encryption with the original key:

Plain Text	9	8	7	6	5	4
Key	0	6	32	9	38	41
Cipher text-1	9	>	W	?	[	]
Key	32	47	6	47	6	32
Cipher Text-2	**Y**	**M**	**]**	**N**	**A**	**}**
Binary equivalent	**0101 1001**	**0110 1101**	**0101 1101**	**0110 1110**	**0110 0001**	**0111 1101**

By flipping a bit of the element A[0][1]= 3(00110011) to(00110001) which is 1

We get the first key as "3 11 32 14 38 41" and second key as "3 41 3 15 3 33"

Encryption with the key with flipped bits:

Plain Text	**9**	**8**	**7**	**6**	**5**	**4**
Key	**3**	**11**	**32**	**14**	**38**	**41**
Cipher text-1	<	**C**	**W**	**D**	**[**	**]**
Key	**3**	**41**	**3**	**15**	**3**	**33**
Cipher Text-2	**?**	**L**	**Z**	**S**	^	`
Binary equivalent	**0011 1111**	**0110 1100**	**0101 1010**	**0101 0011**	**0101 1110**	**0110 0000**

Difference of bits in Cipher Text generated is: 23bits

Avalanche Effect = 23*100/48 = **47.92%**

V. CONCLUSION

Arya A. and Ameta G developed a model for data security. They have used ternary vector and random matrix to generate 2 keys for encryption process. Input text is encrypted two times with the help of generated keys.

This algorithm is advanced version of the model presented by Arya A. and Ameta G. For higher security generation of both the keys have been modified. In the proposed model for removal of repeated values in first key some values are added so that first key does not have multiple repeated values. For generating the second key modified version of rail fence technique is used to achieve higher security. For an intruder it will not be easy to guess the pattern or text.

The proposed model has Avalanche Effect of 47.92% which lies in strict avalanche criteria. It has better avalanche effect than many other algorithms, which provides greater security to data. We are using ternary system with 3 digit number so the length of the first key generated is 27.If we consider ternary vector with four digit number or five digit number then the length of first key will be increased by 34 or 35. Similarly if we consider n-ary vector then the length of the first key can be increase. Longer keys will increase security of our model.

REFERENCES

[1]. Arya A, "2-Key Based Substitution Encryption Model for Cloud Data Storage", International Journal of Research and Scientific Innovation (IJRSI), Volume IV and Issue XII, Dec, 2017

[2]. "Enhancing the performance of Data Encryption Standard algorithm by using Rail Fencing" Ritwik Goyal, Prof. Binod Kumar Mishra, Prashant Lakkadwala, IJRTI, Volume 2, Issue 3,2017

[3]. Akanksha Shukla: "Algorithm for generating sub-keys/basins from a New Substitution Block Cipher Algorithm" International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056 Volume: 03 Issue: 11 | Nov -2016

[4]. Andysah Putera Utama Siahaan, "Rail Fence Cryptography in Securing Information", International Journal of Scientific & Engineering Research, Volume 7, Issue 7, July-2016

[5]. Taranpreet Singh Ruprah, "Advance Encryption and Decryption Technique using Multiple Symmetric Algorithm", Journal of Information Security Research, Volume 7, Number 2, June 2016

[6]. Preeti Poonia and Praveen Kantha, "Comparative Study of Various Substitution and Transposition Encryption Techniques", International Journal of Computer Applications (0975 – 8887), Volume 145 – No.10, July 2016.

[7]. Rajput, Yashpalsingh., Naik, Dnyaneshwar., Mane, Charudatt (2014). An Improved Cryptographic Technique to Encrypt Text using Double Encryption, January.

[8]. Ajit Singh, Aarti Nandal, Swati Malik," Implementation of Caesar Cipher with Rail Fence for Enhancing Data Security" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 12, December 2012

[9]. Balakrishnan.S, Saranya.G, Shobana.S&Karthikeyan.S, "Introducing Effective Third Party Auditing (TPA) for Data Storage Security in Cloud", International Journal of Computer Science and Technology IJCSTVol.2, Issue 2, 2011.

[10]. Omran, S.S.; Al-Khalid, A.S.; Al-Saady, D.M. "A cryptanalytic attack on Vigenere cipher using genetic algorithm", IEEE Conference on Open Systems (ICOS), pp. 59-64, Sep. 2011

[11]. SriramRamanujam, MarimuthuKaruppiah, "Designing an Algorithm with high Avalanche Effect", IJCSNS International

Journal of Computer Science and Network Security, Volume: 11 No.1, pp. 106-111, January 2011

[12]. Omran, S.S.; Al-Khalid, A.S.; Al-Saady, D.M. "Using Genetic Algorithm to Break a Mono-Alphabetic Substitution Cipher", IEEE Conference on Open Systems (ICOS), pp. 63-67, Dec. 2010

[13]. Q. Wang, C. Wang, J. Li, K. Ren, W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing", in Proc. of ESORICS'09, Saint Malo, 2009.

[14]. M. A. Shah, R. Swaminathan, M. Baker, "Privacy preserving audit and extraction of digital contents", Cryptology ePrint Archive, 2008.

[15]. Craig Gentry, Dan Boneh, "Aggregate and verifiably encrypted signatures form bilinear maps", 2004.

[16]. Suter, B.W.; Honeywell, Inc. "The Modular Arithmetic of Arbitrarily Long Sequences of Digits", IEEE Transactions on Computer, Volume: C-23, Issue: 12, pp.1301-1303, Dec. 1974.

[17]. PanditS.N.N, "A New Matrix Calculus", Journal of Society for Industrial and Applied Mathematics, Volume 9, Issue 4, pp. 632-639, Dec., 1961.