DYNAMIC PLAIN CIPHER ALGORITHM

Abstract

This paper aims to review Dynamic Plain Cipher Algorithm .Developed to overcome the disadvantage of RSA, examine its different versions to overcome the weakness of RSA (Rivest Shamir Adleman).RSA is one of the best cryptographic algorithms in use today that ensures secure communication over networks .The Dynamic Plain Cipher Algorithm is developed by Karthik Raja J (3BCA) from SRMArts & ScienceCollege Department of Computer Applications and Technology in 2023 .

Keywords: Public key,Resources,Symmetric key algorithm,ASCII ,cipher text.

Author

J. Karthik Raja
Department of Computer Applications and Technology
SRM Arts & Science College
Chennai, India
karthikraja90804@gmail.com

I. INTRODUCTION

Cryptography is technique of securing information and communications between two or more person from unauthorized user .It is the way of converting the information (plain text) into the collection characters and symbols (cipher text)that are not under stable by person by using the mathematical algorithm. The cipher text is transferred on the internet to the receiver. Then by using the key the cipher text is decoded . The Dynamic Plain Cipher Algorithm is the modified RSA Cryptography algorithm to secure the information over the network with Single key (Public key) for both Encryption and decryption (or) also called as symmetric key . The RSA is a asymmetric cryptographic algorithm mean it use two different key such as public key and private key separately for encryption and decryption. There are three different version are in the Dynamic Plain Cipher Algorithm .The versions has a different level of security to protect the information from unauthorized user .RSA Algorithm may fail sometimes because for complete encryption both symmetric and asymmetric encryption is required and RSA uses asymmetric encryption only. So for the complete encryption the RSA Algorithm is modified to also support the symmetric encryption and named as Dynamic Plain Cipher Algorithm. The Aim of the Dynamic Plain Cipher Algorithm to reduce the cost with high security.

II. EXISTING RSA

It is an asymmetric encryption technique used for secure data transmission especially over the internet .Transmitting confidential and sensitive data over the internet through this technology is safe due to its standard encryption method . The modulus operation playa important role for securing the information. In this algorithm, a code is added to the normal message for security purposes. The algorithm is based on the factorization of large number. Large numbers cannot be easily factorized, so breaking into the message for intruders is difficult.

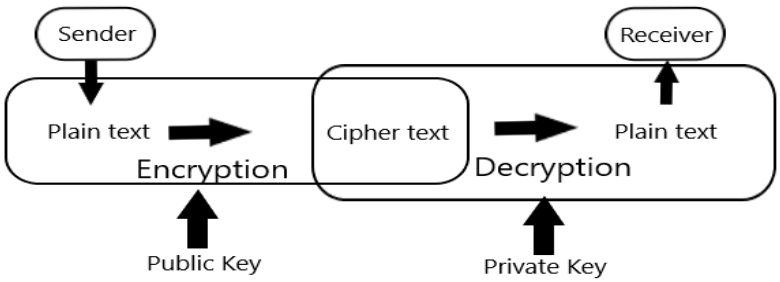


Figure 1: Working of RSA

III. PROPOSED SYSTEM

It is an symmetric encryption technique used for secure data transmission especially over the internet .Transmitting confidential and sensitive data over the internet through this technology is safe due to its standard encryption method . The modulus operation playa important role for securing the information. The all mathematical operation in RSA are also in Dynamic Plain cipher Algorithm . While using single key for both encryption and

decryption it is cheap than asymmetric. It is implemented by changing some formulas in RSA algorithm.

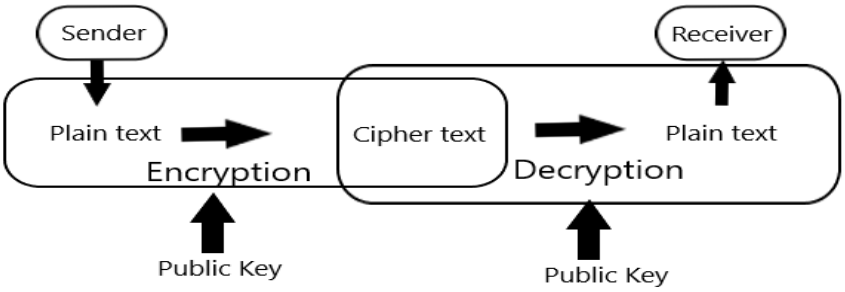


Figure 2: Working of Dynamic Plain Cipher

To Encrypt and Decrypt the data using asymmetric key is more expensive. So , changing some rules in RSA algorithm to support the symmetric key to became as a complete encryption.It is secure than other symmetric cryptography algorithm because it is implemented Symmetric key concept using the same RSA formulas.

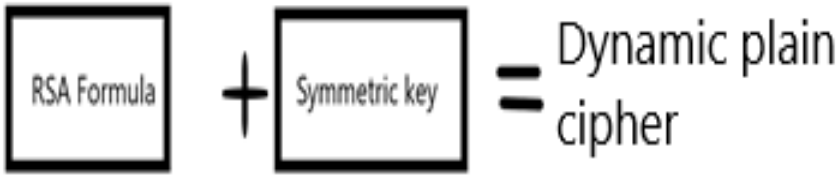


Figure 3: Dynamic Plain Cipher

1. **Resources:** The Two same prime number P and Q are required for the encryption and decryption process .The plain text is also required to generate cipher text

2. **Public key:** This key is used to encrypt and decrypt the information or cipher text .In this Algorithm has two value in the public key are N and E.

   Public Key=[N,E]

   Where N is the multiplication of two prime number P and Q. And E be the value based on the condition $1 < e < \varphi(n)$.The $\varphi(n)$ has be the multiplication of P minus one and Q minus 1 as $\varphi(n)=(p-1)(q-1)$.

IV. VERSION 1

The version 1 itself support the symmetric key encryption but there is no additional security is implemented like changing the cipher text dynamically for each plain text character .The Key [N,E] is used. It is a basic model of dynamic plain cipher algorithm.

1. Formulas:

- N=P*Q.
- p= n mod t ==0 and q= n mod k ==0 where (t!=k , t!=n , k!=t , k!=n).
- φ(n)=(p-1) (q-1).
- Choose e such that 1 < e <φ(n) and e and φ (n) are co-prime.
- l*e mod φ(n)==1 then d=l.
- Encryption :
  c = M^e % n where M=plain text.
- Decryption :
  Plain text= c^d %n.
  Where C=Cipher text

2. Procedures:

- Take two prime number P and Q .Same prime key is must used to decode the cipher text to get the correct plain text otherwise it return the incorrect plain text that is not in understandable form.
  N=P*Q
- Where N is the Multiplication of two prime number P and Q.
  φ(n)=(p-1) (q-1)
- The φ(n) is the multiplication of P minus one and Q minus one .
  1 < E <φ(n)
- The E is the value play a important role to convert the plain text into cipher text in the encryption process .It is the value between the 1 and φ(n).
- Required plain text and public key for the encryption process. In this process it convert the plain text into cipher text that not give meaning to anyone.
  Key=[N,E]
  c = M^e % N
- Where M is the Plain text and by using the above formula the cipher text is calculated and then it is transferred to the receiver.
- It Required cipher text and public key for the decryption process. In this process it convert the cipher text into plain text that give meaning to the receiver.
  Key=[N,E]
  p= n mod t ==0 &
  q= n mod k ==0
- The first step in the decryption process to decode the P and Q value from the data specified in the public key. In the Public key Contains two values N and E .where N is the multiplication of two prime number P and Q . E is the value between 1 and φ(n).
- P and Q are the prime numbers so it not comes in other tables .
- It act as a primary key so using the logic we can easy calculate P and Q from N .
- The N Mod of any Prime Number(T,K) is equal to the o and also satisfy the below condition
  (T!=K , T!=N , K!=T , K!=N).then it taken as P .
- In the same way calculate the Q value also. To Calculate the D value by using the below formula.
  l*e mod φ(n)==1 then d=l

- Where φ(n) is calculated by using the P and Q value . The possible value is calculated and set it as D.
  Plain text= C^d %n
- Where C is the cipher text by using the above formula the plain text is calculated .

3. Example:

- Let Take Two prime number 3 and 11 as
  P=3
  Q=11
- Then F calculate N and φ(n) values by using P and Q as
  N=P*Q
  N=3*11
  N=33
  φ(n)=(P-1)(Q-1)
  φ(n)=(3-1)(11-1)
  φ(n)=(2)(10)
  φ(n)=20
- Calculate The Value of E based on the condition 1 < E <φ(n).E and φ (n) are co-prime.
  1<E<20
- The Value of E must Greater than 1 and lesser than φ(n) .
- So ,Let take E value as 7.
  E=7
- Now the public key is ready to encrypt and decrypt the data.
  Public key=[N,E]
  Public Key=[33,7]
- Encryption
  Key=[33,7]
  M=2
- Where M is the plain text.
- To generate the cipher text for the plain text by using the below formula.
  C = M^E % N
  C=(2)^7 mod 33
- The two power seven is 128.
  C=128 mod 33
  C=29
- The Cipher text is 29 of the plain text 2.
- Decryption:
  Key=[33,7]
  C=29
- Where C is the Cipher text.
- Calculate P and Q value from N by using the formula.
  p= n mod t ==0
  q= n mod k ==0
- If N mod of any prime number give 0 then also the condition is satisfied then the prime number is taken as P.
  (T!=K , T!=N , K!=T , K!=N)

- If T=3 then,P=33 mod 3=0 .The T value is also satisfy the above condition .Then the value of T is taken as P.
  P=3
- As Same way the value of Q is calculated.
  If K=3
  Q=33 mod 3=0
- But K==T so, it not satisfy the condition then change the prime number .
  If K=5
  Q=33 mod 5 =3
- There is a remainder so it not satisfy the condition.
  If K=7 then
  Q=33 mod 7=5
- There is a remainder so it not satisfy the condition.
  If K=11 then
  Q=33 mod 11=0
- The K value is also satisfy the above condition .Then the value of K is taken as Q.
  Q=11
- Calculate the D value by using the bellow formula.
  L*e mod φ(n)==1 then d=L
  φ(n)=(P-1)(Q-1)
  φ(n)=(3-1)(11-1)
  φ(n)=(2)(10)
  φ(n)=20
- Evaluate the φ(n) and E value in the above equation.
  L*7 mod 20==1 then d=L
  Then D=L(L*7 mod 20==1)
  D=3((3*7) mod 20)
  D=3((21) mod 20)
- The 21 mod of 20 is 1 so it satisfy the condition then the value of L is taken as a D.
  D=3(1)
  D=3
- To get the plain text from the cipher text by using the D and N value in the below formula.
  Plain text= C^D %N
  Plain text=29^3 mod 33
  The 29 power of 3 is 24389 .
  Plain text=24389 mod 33
  Plain text=2
- Finally the cipher text 29 is decrypted to plain text 2.

4. Advantages of version 1:

- The Symmetric key encryption is implemented to reduce the cost then Asymmetric key encryption.
- Its secure than other Symmetric Cryptography algorithm .Because it implemented using RSA formula.
- When RSA has both Symmetric and asymmetric encryption is called complete encryption.

V. VRESION 2

In this version has the entire feature of previous version and the dynamic concept .The Key [N,E] is used.

The ASCII values play a important role in this version .The cipher text does not provide any clues to the person because The same two character in the plain text has a different cipher text by using the position of the particular character.So, it is secure then previous and symmetric cryptographic algorithm.

1. Formulas

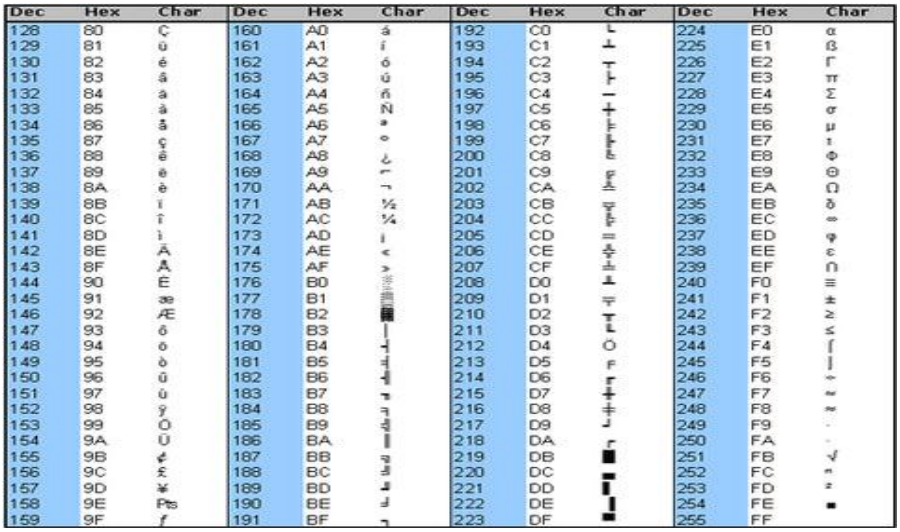
- N=P*Q.
- Pos =M position in the sequence of character.
- p= n mod t ==0 and q= n mod k ==0 where (t!=k , t!=n , k!=t , k!=n).
- φ(n)=(p-1) (q-1).
- Choose e such that 1 < e <φ(n) and e and φ (n) are co-prime.
- l*e mod φ(n)==1 then d=l.
- Encryption
  C1 = M^e % n where M=plain text.
  C=c1 + pos , then convert the cipher value into equivalent ASCII character.
- Decryption
  Convert the cipher value into equivalent ASCII value .
  C1=c - pos .

  Plain text= c1^d %n.
  Where C=Cipher text

2. ASCII: ASCII stand for American Standard Code for Information Interchange, a standard data-encoding format .ASCII assigns standard numeric values to letters, numerals, punctuation marks, and other characters used in computers.

Dec	Hex	Name	Char	Ctrl-char	Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char
0	0	Null	NUL	CTRL-@	32	20	Space	64	40	@	96	60	`
1	1	Start of heading	SOH	CTRL-A	33	21	!	65	41	A	97	61	a
2	2	Start of text	STX	CTRL-B	34	22	"	66	42	B	98	62	b
3	3	End of text	ETX	CTRL-C	35	23	#	67	43	C	99	63	c
4	4	End of xmit	EOT	CTRL-D	36	24	$	68	44	D	100	64	d
5	5	Enquiry	ENQ	CTRL-E	37	25	%	69	45	E	101	65	e
6	6	Acknowledge	ACK	CTRL-F	38	26	&	70	46	F	102	66	f
7	7	Bell	BEL	CTRL-G	39	27	'	71	47	G	103	67	g
8	8	Backspace	BS	CTRL-H	40	28	(	72	48	H	104	68	h
9	9	Horizontal tab	HT	CTRL-I	41	29	)	73	49	I	105	69	i
10	0A	Line feed	LF	CTRL-J	42	2A	*	74	4A	J	106	6A	j
11	0B	Vertical tab	VT	CTRL-K	43	2B	+	75	4B	K	107	6B	k
12	0C	Form feed	FF	CTRL-L	44	2C	,	76	4C	L	108	6C	l
13	0D	Carriage feed	CR	CTRL-M	45	2D	-	77	4D	M	109	6D	m
14	0E	Shift out	SO	CTRL-N	46	2E	.	78	4E	N	110	6E	n
15	0F	Shift in	SI	CTRL-O	47	2F	/	79	4F	O	111	6F	o
16	10	Data line escape	DLE	CTRL-P	48	30	0	80	50	P	112	70	p
17	11	Device control 1	DC1	CTRL-Q	49	31	1	81	51	Q	113	71	q
18	12	Device control 2	DC2	CTRL-R	50	32	2	82	52	R	114	72	r
19	13	Device control 3	DC3	CTRL-S	51	33	3	83	53	S	115	73	s
20	14	Device control 4	DC4	CTRL-T	52	34	4	84	54	T	116	74	t
21	15	Neg acknowledge	NAK	CTRL-U	53	35	5	85	55	U	117	75	u
22	16	Synchronous idle	SYN	CTRL-V	54	36	6	86	56	V	118	76	v
23	17	End of xmit block	ETB	CTRL-W	55	37	7	87	57	W	119	77	w
24	18	Cancel	CAN	CTRL-X	56	38	8	88	58	X	120	78	x
25	19	End of medium	EM	CTRL-Y	57	39	9	89	59	Y	121	79	y
26	1A	Substitute	SUB	CTRL-Z	58	3A	:	90	5A	Z	122	7A	z
27	1B	Escape	ESC	CTRL-[	59	3B	;	91	5B	[	123	7B	{
28	1C	File separator	FS	CTRL-\	60	3C	<	92	5C	\	124	7C	|
29	1D	Group separator	GS	CTRL-]	61	3D	=	93	5D	]	125	7D	}
30	1E	Record separator	RS	CTRL-^	62	3E	>	94	5E	^	126	7E	~
31	1F	Unit separator	US	CTRL-_	63	3F	?	95	5F	_	127	7F	DEL

Figure 4: ASCII Table (0-127)



Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char
128	80	Ç	160	A0	á	192	C0	└	224	E0	α
129	81	ü	161	A1	í	193	C1	┴	225	E1	ß
130	82	é	162	A2	ó	194	C2	┬	226	E2	Γ
131	83	â	163	A3	ú	195	C3	├	227	E3	π
132	84	ä	164	A4	ñ	196	C4	─	228	E4	Σ
133	85	à	165	A5	Ñ	197	C5	┼	229	E5	σ
134	86	å	166	A6	ª	198	C6	╞	230	E6	µ
135	87	ç	167	A7	º	199	C7	╟	231	E7	τ
136	88	ê	168	A8	¿	200	C8	╚	232	E8	Φ
137	89	ë	169	A9	⌐	201	C9	╔	233	E9	Θ
138	8A	è	170	AA	¬	202	CA	╩	234	EA	Ω
139	8B	ï	171	AB	½	203	CB	╦	235	EB	δ
140	8C	î	172	AC	¼	204	CC	╠	236	EC	∞
141	8D	ì	173	AD	¡	205	CD	═	237	ED	φ
142	8E	Ä	174	AE	«	206	CE	╬	238	EE	ε
143	8F	Å	175	AF	»	207	CF	╧	239	EF	∩
144	90	É	176	B0	▒	208	D0	╨	240	F0	≡
145	91	æ	177	B1	▒	209	D1	╤	241	F1	±
146	92	Æ	178	B2	▓	210	D2	╥	242	F2	≥
147	93	ô	179	B3	│	211	D3	╙	243	F3	≤
148	94	ö	180	B4	┤	212	D4	╘	244	F4	⌠
149	95	ò	181	B5	╡	213	D5	╒	245	F5	⌡
150	96	û	182	B6	╢	214	D6	╓	246	F6	÷
151	97	ù	183	B7	╖	215	D7	╫	247	F7	≈
152	98	ÿ	184	B8	╕	216	D8	╪	248	F8	°
153	99	Ö	185	B9	╣	217	D9	┘	249	F9	∙
154	9A	Ü	186	BA	║	218	DA	┌	250	FA	·
155	9B	¢	187	BB	╗	219	DB	▒	251	FB	√
156	9C	£	188	BC	╝	220	DC	▄	252	FC	ⁿ
157	9D	¥	189	BD	╜	221	DD	▌	253	FD	²
158	9E	Pts	190	BE	╛	222	DE	▐	254	FE	■
159	9F	ƒ	191	BF	┐	223	DF	▀	255	FF	

Figure 5: ASCII Table (128-255)

3. Procedure:

- Take two prime number P and Q .Same key is must used to decode the cipher text to get the correct plain text otherwise it return the incorrect plain text that is not in understandable form.
  N=P*Q
- Where N is the Multiplication of two prime number P and Q.
  φ(n)=(p-1) (q-1)
- The φ(n) is the multiplication of P minus one and Q minus one .
  1 < E <φ(n)
- The E is the value play a important role to convert the plain text into cipher text in the encryption process .It is the value between the 1 and φ(n).
- Encryption:
- Required plain text and public key for the encryption process. In this process it convert the plain text into cipher text that not give meaning to anyone.
  Key=[N,E]
  POS=position
- Where POS is the position of a character in the plain text .
  C1 = M^e % N
- After Calculating the cipher value for the plain text add the position for the particular character to achieve the dynamic concept.
  C=C1+POS
- Where M is the Plain text and by using the above formula the cipher text is calculated and then it is transferred to the receiver.
- Decryption:
- It Required cipher text and public key for the decryption process. In this process it convert the cipher text into plain text that give meaning to the receiver.
  POS=position
- Where POS is the position of a character in the cipher text .
  Key=[N,E]
  p= n mod t ==0
  &

q= n mod k ==0

- The first step in the decryption process to decode the P and Q value from the data specified in the public key.
- In the Public key Contains two values N and E .where N is the multiplication of two prime number P and Q . E is the value between 1 and φ(n).
- P and Q are the prime numbers so it not comes in other tables .It act as a primary key so using the logic we can easy calculate P and Q from N .
- The N Mod of any Prime Number(T,K) is equal to the o and also satisfy the below condition
  (T!=K , T!=N , K!=T , K!=N).then it taken as P .
- In the same way calculate the Q value also.
- To Calculate the D value by using the below formula.
  l*e mod φ(n)==1 then d=l
- Where φ(n) is calculated by using the P and Q value . The possible value is calculated and set it as D.
- Minus the position of the character as.
  C=Cn - POS
  Plain text= C^d %n

- Where C is the cipher text by using the above formula the plain text is calculated .

4. Example:

- Let take M = raja.
- Let Take Two prime number 17 and 11 as
  P=17
  Q=11
- Then F calculate N and φ(n) values by using P and Q as
  N=P*Q
  N=17*11
  N=187
  φ(n)=(P-1)(Q-1)
  φ(n)=(17-1)(11-1)
  φ(n)=(16)(10)
  φ(n)=160
- Calculate The Value of E based on the condition 1 < E <φ(n).E and φ (n) are co-prime.
  1<E<160
- The Value of E must Greater than 1 and lesser than φ(n) .
- So ,Let take E value as 7.
  E=7
- Now the public key is ready to encrypt and decrypt the data.
  Public key=[N,E]
  Public Key=[187,7]
- Encryption:
  Key=[187,7]
- Separately convert the each character in the plain text to cipher text .

- The first character of the plain text is ‘r’ .Convert the character into integer value using the
  ASCII table .The Equivalent value for the character r is 114 then. POS is 1
  M=114
  POS=1
- Where M is the Ascii value of the character.
- To generate the cipher text for the plain text by using the below formula.
  C = M^E % N
  C=(114)^7 mod 187
  C=250226879128704 mod 187
  C=126+POS
  C=126+1
  C=127
  Xpos=C
- The Cipher text is 127 of the plain text ‘r’.
- The next character of the plain text is ‘a’ .Convert the character into integer value using the ASCII table .The Equivalent value for the character r is 97 . POS is 2.
  M=97
  POS=2
  C = M^E % N
  C=(97)^7 mod 187
  C=80798284478113 mod 187
  C=92
  C=92+POS
  C=92+2
  C=94
  Xpos=C
- The Cipher text is 94 of the plain text ‘a’.
- The next character of the plain text is ‘j’ .Convert the character into integer value using the ASCII table .The Equivalent value for the character r is 106 . POS is 3,
  M=106
  POS=3
  C = M^E % N
  C=(97)^7 mod 187
  C=150363025899136 mod 187
  C=149+POS
  C=149+3
  C=152
  Xpos=C
- The Cipher text is 152 of the plain text ‘j’.
- The final character of the plain text is ‘a’ .Convert the character into integer value using the ASCII table .The Equivalent value for the character r is 97 .POS is 4.
  M=97
  POS=4
  C = M^E % N
  C=(97)^7 mod 187

C=80798284478113 mod 187
C=92+POS
C=92+4
C=96
Xpos=C

- The Cipher text is 96 of the plain text ‘a’.
- Finally the cipher text of sequence of character is 127 94 152 96 .
- Decryption:
  Key=[187,7]
- Where X is the Cipher text.
- Calculate P and Q value from N by using the formula.
  p= n mod t ==0
  q= n mod k ==0
- If N mod of any prime number give 0 then also the condition is satisfied then the prime number is taken as P.
  (T!=K , T!=N , K!=T , K!=N)
  If T=3 then,
  P=187 mod 3=1
- There is a remainder so it not satisfy the condition.
  If T=5 then,
  P=187 mod 5=2
- There is a remainder so it not satisfy the condition.
  If T=7 then,
  P=187 mod 7=5
- There is a remainder so it not satisfy the condition.
  If T=11 then,
  P=187 mod 11=0
- The T value is also satisfy the above condition .Then the value of T is taken as P.
  P=11
- As Same way the value of Q is calculated.
  If T=3 then,
  P=187 mod 3=1
- There is a remainder so it not satisfy the condition.
  If T=5 then,
  P=187 mod 5=2
- There is a remainder so it not satisfy the condition.
  If T=7 then,
  P=187 mod 7=5
- There is a remainder so it not satisfy the condition.
  If T=11 then,
  P=187 mod 11=0
- If returns 0 but is already choose as a PSo, it not satisfy the condition.
  If K=13
  Q=187 mod 13=5
- There is a remainder so it not satisfy the condition.
  .If K=17 then
  Q=187 mod 17=0

- The K value is also satisfy the above condition .Then the value of K is taken as Q.
  Q=17
- Calculate the D value by using the bellow formula.
  L*e mod φ(n)==1 then d=L
  φ(n)=(P-1)(Q-1)
  φ(n)=(17-1)(11-1)
  φ(n)=(16)(10)
  φ(n)=160
- Evaluate the φ(n) and E value in the above equation.
  L*7 mod 160==1 then d=L
  Then D=L(L*7 mod 160==1)
  D=23((23*7) mod 160)
  D=23((161) mod 160)
- The 161 mod of 160 is 1 so it satisfy the condition then the value of L is taken as a D.
  D=23(1)
  D=23
- To get the plain text from the cipher text by using the D and N value in the below formula.
  Ypos= Xpos^D %N
- The minus the position in Cipher text are
  X1=127-pos=127-1=126
  X2=94-pos=94-2=92
  X3=152-pos=152-3=149
  X4=96-pos=96-4=92
  If pos=1 then
  Y1= X1^D %N
  Y1=126^23 mod 187
  Y1=114
- The Conversion of the value into character using the ASCII is ‘r’ then append it.
  Plain text=’r’
  If pos=2 then
  Y2= X2^D %N
  Y2=92^23 mod 187
  Y1=97
- The Conversion of the value into character using the ASCII is ‘r’ then append it.
  Plain text=’ra’
  If pos=3 then
  Y3= X3^D %N
  Y3=149^23 mod 187
  Y3=106
- The Conversion of the value into character using the ASCII is ‘j’ then append it.
  Plain text=’raj’
  If pos=4 then
  Y4= X4^D %N
  Y4=92^23 mod 187
  Y4=97

- The Conversion of the value into character using the ASCII is ‘a’ then append it. Plain text=’raja’
- Finally the cipher text 127 94 152 96 is decrypted to plain text ‘raja’ (or) 114 97 106 97.

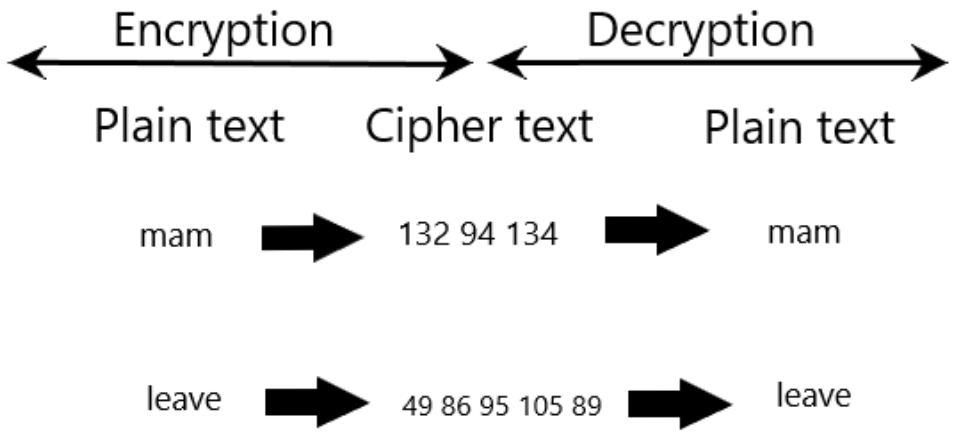


Figure 6: Example of Dynamic Cipher Text

5. Advantages of Version 2:

- It is less expensive than asymmetric cryptographic algorithm.
- It improve security than other Symmetric Cryptography algorithm . Because it implemented using RSA formulas .
- The same character present in the plain text has a different cipher text but in the RSA has the same cipher text.
- The unauthorized usercant identify the relationship of the value or character in the cipher text.

VI. CONCLUSION AND FUTURE ENHANCEMENT

It can replace the current cryptography algorithm used for the less secure data because it cheap and has a high secure .It is the small idea to achieve the RSA as a complete encryption algorithm then only we use this algorithm for both high secure and low secure data with different cost. Cryptography **i**s the study of encrypting and decrypting data to prevent unauthorized access like inception, modification etc.. The cipher text should be known by both the sender and the receiver. cryptography allows for the secure transmission of digital data between willing parties. It is used to safeguard company secrets, secure classified information, and sensitive information from fraudulent activity, among other things. Crypto means hidden and graph means writing .In future to increase the security the dynamic concept is apply for each character without changing the same two primary number. And also reduce the processing time and improve the performance. This algorithm is also implemented in the messaging software.

