Fuzzy Systems and Soft Computing
ISSN : 1819-4362

IMPLEMENTATION OF DYNAMIC PLAIN CIPHER ALGORITHM IN KIVY MESSAGER

Dr. V. S. Padmavathy Assistant Professor, Department of Computer Applications and Technology, SRM Arts and Science College E-mail: vspadmavathy@gmail.com
J. Karthik Raja Student, Dept of Computer Applications and Technology, SRM Arts and Science College

Abstract

A varied range of messenger applications are available for exchanging the data over the internet. Privacy is always a major issue when it comes to the usage of the free service. Thus it has to be protected by using the encryption techniques in order to the store the information confidentially as well as from unauthorized access. This paper proposes a hybrid algorithm by implementing the Dynamic Plain Cipher algorithm with the Kivy Messenger.The goal of the DPC (Dynamic Plain Cipher) Algorithm is to encrypt and decrypt information in a cost-efficient manner. Kivy Messenger is an Android application for communication. The DPC supports static and dynamic encryption and decryption. The DPC Algorithm is special because it doesn't require any dedicated server for processing.

Keywords—
Message Encryption, Android, Security, Cryptography, Public Key, Authentication, Kivy Messager, Dynamic Character Set.. Etc.

1. INTRODUCTION

Kivy Messenger is an Android application developed using the Python Kivy module. With the help of Bulldozer, the Python program is converted to an APK (.py to .apk). Python Kivy is a framework for developing mobile and Android applications. Not only for APKs, but using PyInstaller, conversion of the Python Colle program to an EXE can be done. Cryptography is a technique used to secure the transfer of information from one user to another, preventing unauthorized access.

[1]R. L. Rivest et al developed a RSA algorithm to replace the National Bureau of Standards Algorithm due to less secure of data. RSA implements a public key cryptosystem that means it is a asymmetric cryptography algorithm and it uses two different key for encryption and decryption.[2] Omar G. Abood et al discusses the various symmetric and asymmetric cryptographic algorithms. A cryptographic procedure that requires two keys—one hidden and the other public—is referred to as symmetric key cryptography. [3] Christophe De Cannière et al discusses about the blowfish algorithm. Bruce Schneier created the 64-bit block cipher known as Blowfish, which was released in 1994. It was meant to be a compelling substitute for IDEA or DES . .This Blowfish algorithm is designed and developed to increase the security for data and performance. [4] Dwi Yuny SYLFANIA et al integrated the RSA and Blowfish algorithms into the Android application-based email sending and receiving process. According to the study's findings, the Blowfish algorithm is more quick than the RSA algorithm. [5] Nurhayati et al explains how results are being utilized to design and develop an instant messaging program for the Android mobile platform that can both encrypt and decrypt text messages in order to improve security features on instant messaging apps.

[6] S Behera et al discusses that Today's chat apps are all utilized for sending messages fast and safely. Actually, things are not as secure as they seem when it comes to the sent messages. Therefore, in order to close this gap, homomorphic encryption is employed in this research to more protect the messages without slowing down the transaction. The purpose of this work is to create a homomorphic encryption chat application, which provides an extra layer of security on top of end-to-end encryption. [7] Ashok Kumar Nanda et al have examined the NTRUSign (NTRU Signature) algorithm and the Number Theory Research Unit (NTRU) Crypto algorithm in this work. A theoretical comparison of NTRU and RSA's performance parameters, like memory space, speed, efficiency, is done. [8] Ammar Hammad Alet al offers a recommendation for an end-to-end encrypted secure chat software for Android-powered handsets. This is made feasible by the use of

public key cryptography algorithms. Elliptic Curve Diffie Hellman Key Exchange (ECDH) algorithm-based symmetric data encryption was accomplished by the proposed application by generating the key pair and exchanging it for a shared key. The suggested program allows users to communicate via text, photo, and voice.

The Dynamic Plain Cipher algorithm is a symmetric key cryptography algorithm, where in a specific public key is used for encryption as well as decryption. The main advantage of this algorithm is that when the same P and Q are used to encrypt the same plaintext, it returns different cipher text each time. This occurs by using the Dynamic Character Set. Another subtype of this algorithm applies the dynamic character set to each character in the plaintext. The Dynamic Plain Cipher algorithm is an updated or modified type of the RSA algorithm. The RSA algorithm is an asymmetric cryptography algorithm, requiring both public and private keys for encryption and decryption. If the same P and Q are used to encrypt the same plaintext in RSA, it returns the same cipher text.

2. EXISTING RSA

RSA stands for Rivest, Shamir, Adleman. It is one of the asymmetric cryptography algorithms. Here the encryption of the plaintext is done by the public key. The Private key plays a major role in the decryption process.RSA is considered the best algorithm for securing information.

There is no way to encrypt and decrypt information or plaintext using the public key alone. While using both the public and private keys to secure information is effective, it can be costly. Encrypting and decrypting plaintext using the same P and Q values results in the same cipher text, as the structure of RSA is static.

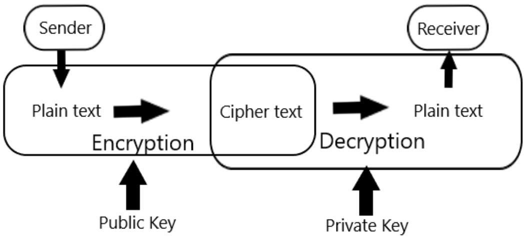


Fig.1. Structure Of RSA

The above diagram explain the structure of Asymmetric cryptography algorithm.

3. PROPOSED SYSTEM

The DPC stands for Dynamic Plain Cipher Algorithm . It is developed to overcome the disadvantages of RSA. DPC is a Symmetric key cryptography algorithm that means it uses a single Public key for both encryption and decryption. So its cost efficient way to secure the information .It has the dynamic concept that done by using the dynamic character set “ If the same information is encrypted and decryption by using the same P and Q value then it return different cipher text for each time.

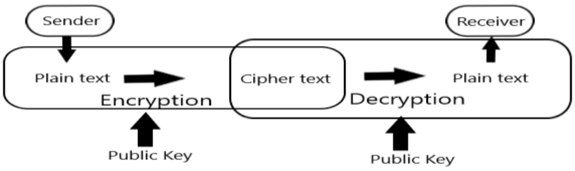


Fig.2. Working Of Dynamic Plain Cipher

The ideal to secure the information with low key bit because while using the high key bit it increase the processing time and also it has a static value so using the dynamic character set to implement the dynamic value for each time so by replacing the character it gives the infinite cipher text for each encryption of the value.

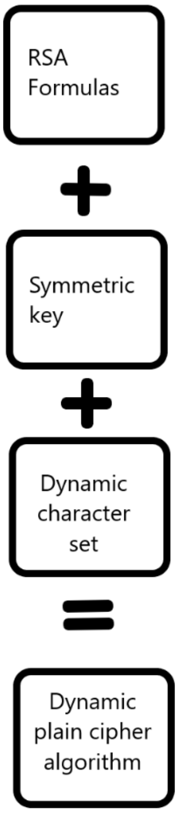


Fig.3. Structure Of DPC

It uses a single key for both encryption and decryption (public key). Its cost is lesser then the Asymmetric encryption. This cryptography algorithm is implemented in the Kivy messager application and the software doesn't have any dedicated server.

4. RESOURCES

To implement this Dynamic Plain Cipher Algorithm required three values P , Q and R. Where P and Q are the prime number and R is the random number to implement the dynamic concept.

4.1 PUBLIC KEY

The Dynamic plain cipher algorithm is a Symmetric key algorithm in cryptography. So it only need single key for both encryption and decryption is public key.

Public Key For DPC is =[N,E]

Where N represent the product of two prime number P and Q. E represent the value taken based on the condition .

$1 < E < \varphi(n)$.

$\varphi(n)$ represent multiplication of P minus one and Q minus 1 as

$\varphi(n)=(P-1)(Q-1)$.

4.2 FORMULAS

The symmetric key encryption is achieved by changing some formulas in the RSA Algorithm . RSA is Asymmetric algorithm so it requires two as Public key for encryption and for decryption Private key . The formulas play a important role to achieve the Symmetric key so Dynamic plain Cipher Algorithm only required single key (public key) for both encryption and decryption.

1. N=(P*Q) → N is the product of two prime number P and Q .P= N mod T ==0 and Q= N mod K ==0 where Condition is (T!=K , T!=N , K!=T , K!=N). → P and Q value are calculated by using the MOD with N and any prime number . This Process done in the decryption stage.
2. $\varphi(N)=(P-1)(Q-1)$. → $\varphi(n)$ is represent the product of P minus 1(P-1) and Q minus 1 (Q-1). This value using
3. $E= 1 < E < \varphi(N)$
4. $D=(L*E \bmod \varphi(N)==1)$
5. Encryption

   -1<R<N

G=(R+C)Mod S

RC=Character set (R mod S)

M^E % N

6. Decryption

C^D % N.

7. R=RN MOD DC or RN % CD

RN→ Random Number

DC → Size of Dynamic character set

4.3 PROCEDURE

The first step of the Dynamic plain cipher algorithm to choose two prime number P and Q . P → prime number(1)

Q → prime number(2)

N = P * Q

Where N is the product of two prime number choose in the previous stage. If any wrong prime number is taken then in the decryption return wrong plain text that meaningless.

φ(N)=(P-1) (Q-1)

Where φ(P*Q) or φ(N) represent the product of P-1 and Q-1.

1 < E < φ(N)

The E value is taken based on the above condition (E>1 and φ(N) >E).

Encryption:

For encryption we need two things plain text or information to encrypt and public key.

Public Key=[N,E]

Plain text (or) M= information

In The end of the process the cipher text is generated for the given plaintext .

c = M^e % N

Where M represent the Plain text, E is the value in the public key and N also present in the public key . The above formula is used to generate the cipher text or encrypted plain text .

To implement the dynamic concept the R value is calculated that is nothing but the random unique number to perform the dynamic concept..

-1<R<N

R=Random number.

The R value Must greater then -1 and lesser then N .

Now We need the any size of character set . character set contain the collection of various character or string of character.

The each element in the character set may be unary ,binary,……etc.

It also contain numbers and special symbols example “#,57,*9”

Example .

a=['aA', 'bB', 'cC', 'dD', 'eE', 'fF', 'gG', 'hH', 'iI', 'jJ', 'kK', 'lL', 'mM', 'nN', 'oO', 'pP', 'qQ', 'rR', 'sS', 'tT', 'uU', 'vV', 'wW', 'xX', 'yY', 'zZ','1A', '1B', '1C', '1D', '1E', '1F', '1G', '1H', '1I', '1J', '1K', '1L', '1M', '1N', '1O', '1P', '1Q', '1R', '1S', '1T', '1U', '1V', '1W', '1X', '1Y', '1Z','a1','q2','w3','r4','e5','t6','y7','i8','o9','p0','2a', '2b', '2c', '2d', '2e', '2f', '2g', '2h', '2i', '2j', '2k', '2l', '2m', '2n', '2o', '2p', '2q', '2r', '2s', '2t', '2u', '2v', '2w', '2x', '2y', '2z','3A', '3B', '3C', '3D', '3E', '3F', '3G', '3H', '3I', '3J']

G=(R+C)Mod S

Now To calculate the Cipher text add the R value with C.

Where R is a Random number and C is the Cipher text In number. The R value must less then or equal to size of character set it is done by using the bellow formula.

Where S is the Size of the Character set .

By using the Mod operator it return the value with in the size of character set.Find the character in the character set in the position of the G value.

RC=Character set (R mod S)

As the same process the RC character is calculated and Bind to the front of the cipher text.

Then the value taken from the character set is the cipher text using for the encrypted plaintext.

Decryption:

For decryption it requires both key and cipher text or encrypted plaintext that is meaningless. The Dynamic Plain Cipher Algorithm is a Symmetric key cryptography algorithm so it use same key for both encryption and decryption . The public key contain two values N (Product of P and Q) and E. After reviving the public key we need to start the decryption process .

DPC Public Key=[N,E]

The first step is to calculate the Two prime number which is used to generate the public key .

P= (N MOD X) ==0

The P value is calculated by using the Mod operator by using the criteria the two values are prime number so if N mod of any prime number is 0 then its is taken as a P value.

Q= (N MOD Y) ==0

X and Y represent the any prime number.

As Same as P the Q value is calculated by using the Mod operator by using the criteria the two values are prime number so if N mod of any prime number is 0 then its is taken as a P value.

P and Q are two prime numbers so it not comes in other multiplication tables then it act as a primary key so

Based on the concept we an calculate the P and Q from N by using the Mod Operator.

If the prime numbers are calculated, they must also satisfy the below condition to avoid duplication.

(X!=Y , X!=N , Y!=X , Y!=N)

U*E mod φ(N)==1

The D value is calculated by using the above formula in it E value present in the public key and φ(N) value is calculated by using the p and Q .

φ(N)=(P-1) * (Q-1)

D=(L*E mod φ(N)==1)

Where φ(P*Q) or φ(N) represent the product of P-1 and Q-1.

If multiplication of any number to E Mod of φ(N) is equal to 1 then the value is taken as a D.

The R value present in the cipher text as first character or string using the character to find the index position in the character set and assign the value to R. The C value is calculate by reversing the encryption process .

Find the position or index that the cipher character present in the character set and minus the R value and assign that to C.

C=V-R

a=['aA', 'bB', 'cC', 'dD', 'eE', 'fF', 'gG', 'hH', 'iI', 'jJ', 'kK', 'lL', 'mM', 'nN', 'oO', 'pP', 'qQ', 'rR', 'sS', 'tT', 'uU', 'vV', 'wW', 'xX', 'yY', 'zZ','1A', '1B', '1C', '1D', '1E', '1F', '1G', '1H', '1I', '1J', '1K', '1L', '1M', '1N', '1O', '1P', '1Q', '1R', '1S', '1T', '1U', '1V', '1W', '1X', '1Y', '1Z','a1','q2','w3','r4','e5','t6','y7','i8','o9','p0','2a', '2b', '2c', '2d', '2e', '2f', '2g', '2h', '2i', '2j', '2k', '2l', '2m', '2n', '2o', '2p', '2q', '2r', '2s', '2t', '2u', '2v', '2w', '2x', '2y', '2z','3A', '3B', '3C', '3D', '3E', '3F', '3G', '3H', '3I', '3J']

Now, All the resource are ready to perform the decryption process.

Plain text= (C^D) %N

Where C represent the cipher text which is calculated during the Encryption process it is nothing but the encrypted plain text .

Finally , By using the above formula the plain text or information that is calculated from the cipher text which is calculated during the encryption process.

4.4 EXAMPLE

1. Let Encrypt and decrypt the plain text “4” by using Dynamic Plain Cipher Algorithm.

Given:

Plain Text =4

The Plain Text In the Integer Form so directly taken it as plain text.

Take two prime number 17 and 11 for P and Q.

P=17

Q=11

Calculate the N value

N=P*Q

Where N is the product of two prime number P and Q.

N=17*11

N=187

Calculate the φ(N) is nothing but the product or P-1 and Q-1 .

φ(n)=(P-1) *(Q-1)

φ(n)=(17-1)*(11-1)

φ(n)=(16*10)

φ(n)=160

Calculate the E value which play a major role during encrypting and decryption the plain text.

1 < E < φ(N)

If The E value must greater then 1 and also lesser then the φ(n) or 160.Let Take the 3 as E.

1 < 3 < 160

The above condition is satisfy because the value of E =3 is greater then the 1 and its lesser then φ(n) or 160.

Now Create a public key because all values required for key is available.

Public Key=[N,E]

Where N is the product of two prime number and The E represent the value which is lesser then φ(n) and greater then 1.

Public key of DPC =[187,3]

Encryption :

Taken a positive number as R.

-1<R<N

Where R is the Random number and N is the product of two prime number present in the Public key. The R value Must greater then -1 and lesser then N .

C = ME % N

Where M is the plain text and N is the product of two prime number .

c = 43 % 187

c= 64 % 187

c=64

-1<R<N

Take the number between -1 and N.

R=5

G=(R+C)Mod S

Calculate the G value by using R, C and s.

The Size of the character set is 129 so

S=129

G=(5+64) Mod 129

G=69 Mod 129

G=69

Now We need get the character from character set by using the G value as

Cipher text= Character Set (R) + Character Set (G)

Character Set (69) = 2h

The Cipher text is fF2h for the plain text 4.

Cipher Text = fF2h

Decryption :

DPC Public Key=[187,3]

Calculate P and Q value using public key.

P= (N MOD X) ==0

If any prime number satisfy the above condition then taken it as P and also satisfy the below condition .

(X!=Y , X!=N , Y!=X , Y!=N)

P= (187 MOD X) ==0

If X=2 then

P= (187 MOD 2)

P=1

P!=0

If X=3 then

P= (187 MOD 3)

P=1

P!=0

If X=5 then

P= (187 MOD 5)

P=2

P!=0

If X=7 then

P= (187 MOD 7)

P=5

P!=0

If X=11 then

P= (187 MOD 11)

P=0

The condition is satisfy so take the prime number as P

P=11

In the same way calculate the Q value .

Q= (187 MOD Y) ==0

If Y=2 then

Q= (187 MOD 2)

Q=1

Q!=0

If Y=3 then

Q= (187 MOD 3)

Q=1

Q!=0

If Y=5 then

Q= (187 MOD 5)

Q=2

Q!=0

If Y=7 then

Q= (187 MOD 7)

Q=5

Q!=0

If Y=11 then

Q= (187 MOD 11)

Q=0

But P=Q

If Y=13 then

Q= (187 MOD 13)

Q=5

Q!=0

If Y=17 then

Q= (187 MOD 17)

Q=0

Q=0

The condition is satisfy so take the prime number as Q as

Q=17

The Two prime number are calculated from the N value .

φ(n)=(P-1) *(Q-1)

Now calculate the value for φ(n) by using the above formula.

φ(n)=(P-1) *(Q-1)

φ(n)=(11 -1) *(17-1)

φ(n)=(10) *(16)

φ(n)=160

D=(L*E mod φ(N)==1)

If multiplication of any number into E Mod of φ(N) is equal to 1 then the value is taken as a D.

D=(107*3 mod 160)

D=1

D==1

So take the value as D=107

Cipher Text = fF37

The First value in the cipher text Represent the R value .

Calculate the R value by using the first two character of the cipher text.

The character set is

a=['aA', 'bB', 'cC', 'dD', 'eE', 'fF', 'gG', 'hH', 'iI', 'jJ', 'kK', 'lL', 'mM', 'nN', 'oO', 'pP', 'qQ', 'rR', 'sS', 'tT', 'uU', 'vV', 'wW', 'xX', 'yY', 'zZ','1A', '1B', '1C', '1D', '1E', '1F', '1G', '1H', '1I', '1J', '1K', '1L', '1M', '1N', '1O', '1P', '1Q', '1R', '1S', '1T', '1U', '1V', '1W', '1X', '1Y', '1Z','a1','q2','w3','r4','e5','t6','y7','i8','o9','p0','2a', '2b', '2c', '2d', '2e', '2f', '2g', '2h', '2i', '2j', '2k', '2l', '2m', '2n', '2o', '2p', '2q', '2r', '2s', '2t', '2u', '2v', '2w', '2x', '2y', '2z','3A', '3B', '3C', '3D', '3E', '3F', '3G', '3H', '3I', '3J', '3K', '3L', '3M', '3N', '3O', '3P', '3Q', '3R', '3S', '3T', '3U', '3V', '3W', '3X', '3Y', '3Z','31','32','33','34','35','36','37','38','39','30','4a', '4b', '4c', '4d', '4e']

R=character set(fF)

R=5

F= character set(2h)

Calculate the F value by using the cipher text.

F=69

C=F-R

C=69-5

C=64

Finally all resources are available so now decrypt the cipher text.

Plain text = Cd % n.

Plain text=64^107 Mod 187

Plain Text= 4

The Plain text 4 in calculated from the cipher text fF2h.

2. Let Encrypt and decrypt the plain text “i” by using Two prime number 11 and 17 in Dynamic Plain Text

Given:

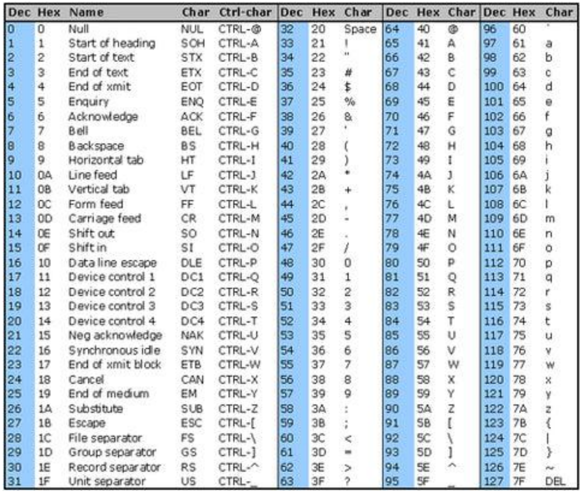
Plain Text =ASCII(i)=107

If the given text in alphanumeric then convert it into integer by using the ASCII Table .

The Ascii value of character “i” is 107.

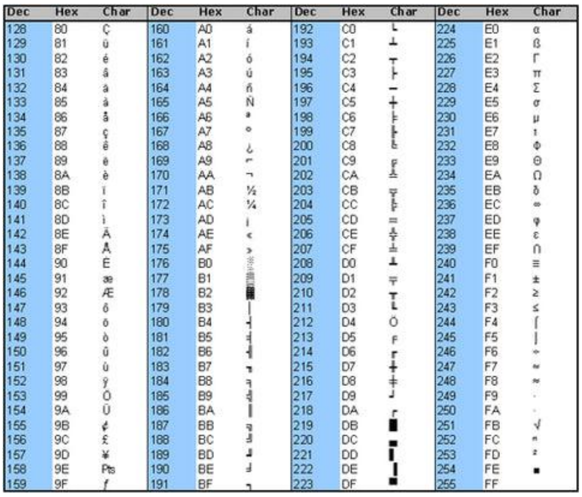
Take two prime number 17 and 11 for P and Q.

P=17 Q=11



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

Fig.4. Ascii Table



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	Ö	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	

Fig.5. Ascii Table

Calculate the N value

$N=P*Q$

Where N is the product of two prime number P and Q.

$N=17*11$

$N=187$

Calculate the φ(N) is nothing but the product or P-1 and Q-1 .

$\varphi(n)=(P-1) *(Q-1)$

$\varphi(n)=(17-1)*(11-1)$

$\varphi(n)=(16*10)$

$\varphi(n)=160$

Calculate the E value which play a major role during encrypting and decryption the plain text.

$1 < E < \varphi(N)$

If The E value must greater then 1 and also lesser then the φ(n) or 160.Let Take the 7 as E.

$1 < 7 < 160$

The above condition is satisfy because the value of E =7 is greater then the 1 and its lesser then φ(n) or 160.

Now Create a public key because all values required for key is available.

Public Key=[N,E]

Where N is the product of two prime number and The E represent the value which is lesser then φ(n) and greater then 1.

Public key of DPC =[187,7]

Encryption :

Take a positive number as R.

$-1<R<N$

Where R is the Random number and N is the product of two prime number present in the Public key. The R value Must greater then -1 and lesser then N .

C = ME % N

Where M is the plain text and N is the product of two prime number .

c = 1057 % 187

c= 140710042265625 % 187

c=96

-1<R<N

Take the number between -1 and N.

R=10

G=(R+C)Mod S

Calculate the G value by using R, C and s.

The Size of the character set is 129 so

S=129

G=(10+96) Mod 129

G=106 Mod 129

G=106

Now We need get the character from character set by using the G value as

Cipher text= Character Set (R) + Character Set (G)

Character Set (106) = 3S

The Cipher text is kK3S for the plain text 4.

Cipher Text = kK3S

Decryption :

DPC Public Key=[187,7]

Calculate P and Q value using public key.

P= (N MOD X) ==0

If any prime number satisfy the above condition then taken it as P and also satisfy the below condition .

(X!=Y , X!=N , Y!=X , Y!=N)

P= (187 MOD X) ==0

If X=2 then

P= (187 MOD 2)

P=1

P!=0

If X=3 then

P= (187 MOD 3)

P=1

P!=0

If X=5 then

P= (187 MOD 5)

P=2

P!=0

If X=7 then

P= (187 MOD 7)

P=5

P!=0

If X=11 then

P= (187 MOD 11)

P=0

The condition is satisfy so take the prime number as P

P=11

In the same way calculate the Q value .

Q= (187 MOD Y) ==0

If Y=2 then

Q= (187 MOD 2)
Q=1
Q!=0
If Y=3 then
Q= (187 MOD 3)
Q=1
Q!=0
If Y=5 then
Q= (187 MOD 5)
Q=2
Q!=0
If Y=7 then
Q= (187 MOD 7)
Q=5
Q!=0
If Y=11 then
Q= (187 MOD 11)
Q=0
But P=Q
If Y=13 then
Q= (187 MOD 13)
Q=5
Q!=0
If Y=17 then
Q= (187 MOD 17)
Q=0
Q=0
The condition is satisfy so take the prime number as Q as

Q=17

The Two prime number are calculated from the N value .
φ(n)=(P-1) *(Q-1)
Now calculate the value for φ(n) by using the above formula.
φ(n)=(P-1) *(Q-1)
φ(n)=(11 -1) *(17-1)
φ(n)=(10) *(16)
φ(n)=160
D=(L*E mod φ(N)==1)
If multiplication of any number into E Mod of φ(N) is equal to 1 then the value is taken as a D.
D=(23*7 mod 160)
D=1
D==1
So take the value as D=23
Cipher Text = kK3S
The First value in the cipher text Represent the R value .
Calculate the R value by using the first two character of the cipher text.
The character set is
a=['aA', 'bB', 'cC', 'dD', 'eE', 'fF', 'gG', 'hH', 'iI', 'jJ', 'kK', 'lL', 'mM', 'nN', 'oO', 'pP', 'qQ', 'rR', 'sS', 'tT', 'uU', 'vV', 'wW', 'xX', 'yY', 'zZ','1A', '1B', '1C', '1D', '1E', '1F', '1G', '1H', '1I', '1J', '1K', '1L', '1M', '1N', '1O', '1P', '1Q', '1R', '1S', '1T', '1U', '1V', '1W', '1X', '1Y', '1Z','a1','q2','w3','r4','e5','t6','y7','i8','o9','p0','2a', '2b', '2c', '2d', '2e', '2f', '2g', '2h', '2i', '2j', '2k', '2l', '2m', '2n', '2o', '2p', '2q', '2r', '2s', '2t', '2u', '2v', '2w', '2x', '2y', '2z','3A', '3B', '3C', '3D', '3E', '3F', '3G', '3H',

'3I', '3J', '3K', '3L', '3M', '3N', '3O', '3P', '3Q', '3R', '3S', '3T', '3U', '3V', '3W', '3X', '3Y', '3Z','31','32','33','34','35','36','37','38','39','30','4a', '4b', '4c', '4d', '4e']

R=character set(kK)

R=10

F= character set(3S)

Calculate the F value by using the cipher text.

F=106

C=F-R

C=106-10

C=96

Finally all resources are available so now decrypt the cipher text.

Plain text = Cd % n.

Plain text=96^23 Mod 187

Plain Text= 105

Plain text=Ascii(105)

Plain text=i

The Plain text 105 or ASCII(i) in calculated from the cipher text kK3S

5 KIVY MESSENGER

Kivy Messenger is an Android application developed to transfer information from one mobile device to another over the internet.

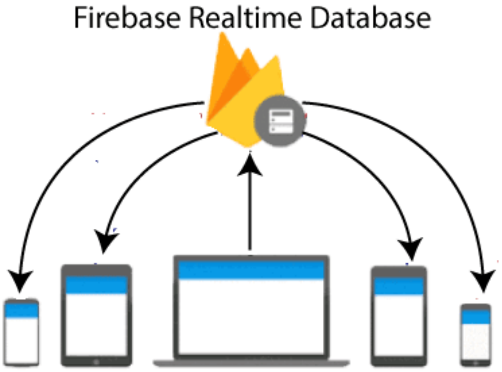


Fig.6. Firebase Real-Time Database

This software uses the Firebase database to store the necessary information

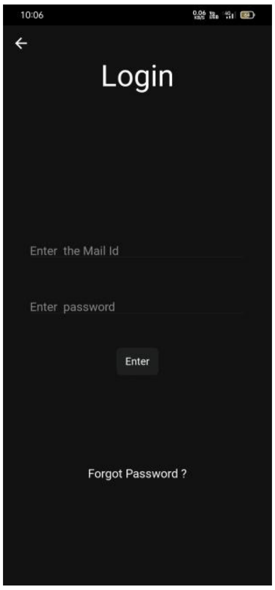


Fig.7. Login Page

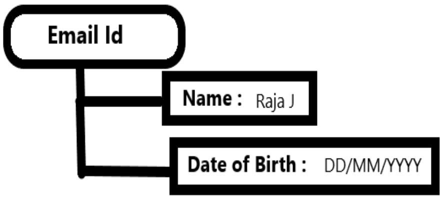


Fig.8. Database Structure

Authentication is done using the Python smtplib module, which employs the Simple Mail Transfer Protocol. There is no dedicated server for this software, so the authentication process is carried out on their mobile or devices.

6 RESULTS

The Dynamic Plain Cipher Algorithm is developed specifically for the Kivy message to reduce costs, maintenance, and improve performance. The Kivy message uses an email ID for authentication because in the future, the physical SIM slot may not be available for mobile allocation. The Dynamic Plain Cipher Algorithm is a straightforward cryptography algorithm.Dynamic Plain Cipher is the updated version of RSA, supporting public key for both encryption and decryption. Therefore, RSA is now considered a complete encryption algorithm.

In this software, a custom Dynamic Plain Cipher Algorithm is implemented for better performance and cost efficiency.

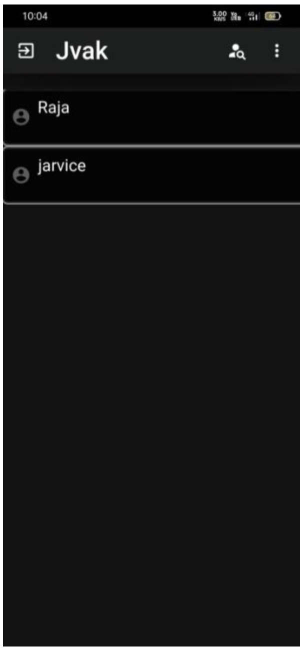


Fig.9. Main Page Of Kivy Messager

The above image shows the main page of the key application that contains two users, Raja and Jarvis, on the account of one authorized person. This type of data is stored in the real-time database. This application allows an infinite number of users. Each user is authorized by using their email with the help of the Smtplib Python module.

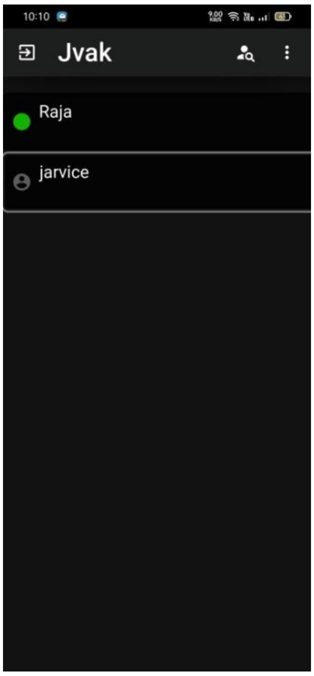
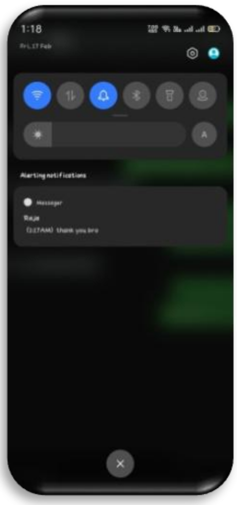


Fig.9. Pop Message

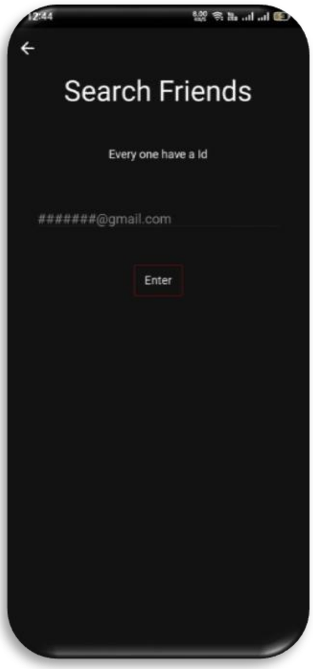
In the above image, the green dot specifies that some messages have been received from a particular user. Additionally, this software pushes notifications for each message received from other users using the notification manager.



Raja
(1:17AM) thank you bro

Fig.10. Notification

The notification is displayed using the Python Plyer module. Plyer is developed to run on Android as well. The notification is displayed using the Python Plyer module. Plyer is developed to run on Android as well. The toolbar has three buttons: Exit button, user search option, and settings button.



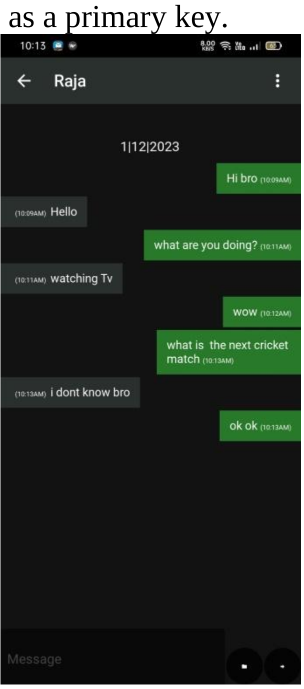
Every one have a Id

#######@gmail.com

Fig.11. Search User

Search a Friend using their mail id.

Upon clicking the enter button, the request goes to search in the database. If it is present, it displays the 'Add' button to start communication. Otherwise, it displays a warning message using the dialog class. Using exception handling, the problem is identified and a warning message is displayed based on the issue.The user search option is used to find a valid user and establish a relationship with them. This search process is performed using the email address.The email address plays an important role in the Kivy messaging software, acting as a primary key.



1|12|2023

Hi bro (10:09AM)

(10:09AM) Hello

what are you doing? (10:11AM)

(10:11AM) watching Tv

wow (10:12AM)

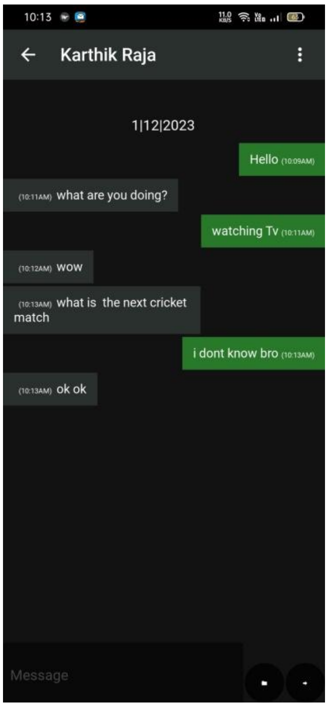
what is the next cricket match (10:13AM)

(10:13AM) i dont know bro

ok ok (10:13AM)

Fig.12. User 1 Message Page

The Message Screen class is added to the screen manager based on the total number of relationships per object. In the particular class, many Grid layouts are declared and initialized as nested layouts. The Top-Bar contains the person's name and two action buttons in opposite directions. The arrow button is used to navigate to the previous class, and the three-dot button is used to view the particular person's details. At the bottom or lowest layout, three classes are present: Text-Input, IconButton1, and IconButton2. IconButton2 is used to send messages to the particular person using an algorithm.


10:13

Karthik Raja

1|12|2023

Hello (10:09AM)

(10:11AM) what are you doing?

watching Tv (10:11AM)

(10:12AM) wow

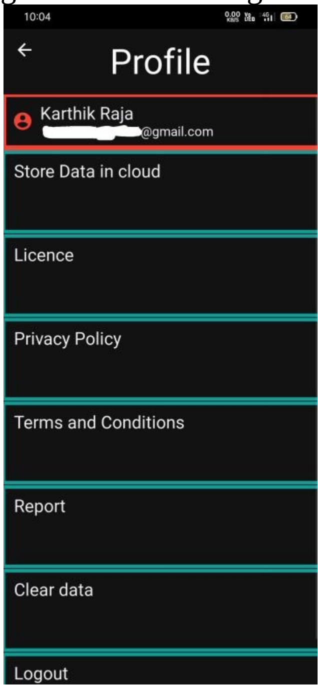
(10:13AM) what is the next cricket match

i dont know bro (10:13AM)

(10:13AM) ok ok

Message

Fig.13. User 2 Message Page


10:04

Profile

Karthik Raja
[redacted]@gmail.com

Store Data in cloud

Licence

Privacy Policy

Terms and Conditions

Report

Clear data

Logout

Fig.13. User Settings Page

The username and email ID of the account are displayed on the screen. Many services are provided in the profile (or) settings.Cloud storage is used to store the relationships in the cloud. When logging into an account, it displays the relationships.The terms and conditions and privacy policy are provided in the application. Clear data is used to clean all chat messages from every person. Logging out is used to logout or leave the current account. On-click, it clears the data and goes to the login screen.

7 CONCLUSION

The Dynamic Plain Cipher Algorithm is a modified version of RSA. DPC cryptography algorithm combines the RSA formula, symmetric key, and dynamic character set. The algorithm is designed in the Kivy Messenger Application to handle all processes, such as database updating and user verification, which is done manually by raising requests to the server. This software uses client-server architecture to transfer information between users. The Dynamic Plain Cipher Algorithm employs a variable-sized character set. However, the character set must contain a large number of characters or elements for security purposes. Using a small character set could make it easier for unauthorized users to crack the character set. Authentication is performed using the Python SMTPLIB module by sending a One-Time Password (OTP) to the given email address. Encryption and decryption in the Dynamic Plain Cipher Algorithm take place within 0.5 to 1.5 seconds, depending on the prime number chosen during encryption, which affects the time duration.

REFERENCES

1. R. L. Rivest, A. Shamir and L. Adleman, “A Method for Obtaining Digital Signature and Public-Key Cryptosystems,” Communications of the ACM, Vol. 21, No. 2, 1978, pp. 120-126.

2. Omar G. Abood, Shawkat K. Guirguis,”A Survey on Cryptography Algorithms”, International Journal of Scientific and Research Publications, Volume 8, Issue 7, July 2018

3. International Journal of Scientific and Research Publications, Volume 8, Issue 7, July2018,ISSN 2250-3153

4. Christophe De Cannière , Encyclopedia of Cryptography and Security

5. Dwi Yuny SYLFANIA , Fransiskus Panca JUNIAWAN , LAURENTINUS , and Harrizki Arie PRADANA,” Blowfish–RSA Comparison Analysis of the Encrypt Decrypt Process in Android-Based Email Application”, Advances in Intelligent Systems Research, volume 172.

6. Nurhayati; Kastari; Feri Fahrianto ,“End-To-End Encryption on the Instant Messaging Application Based Android using AES Cryptography Algorithm to a Text Message”, 10th International Conference on Cyber and IT Service Management (CITSM)

7. S Behera, A Kanth, AA Suresh, CVR Ashwin, JRPrathuri,”Chat Application Using Homomorphic Encryption”, Fourth International Conference on Advances in Electrical and Computer Technologies 2022 (ICAECT 2022)

8. Ashok Kumar Nanda & Lalit Kumar Awasthi “A Proposal for SMS Security Using NTRU Cryptosystem”, International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness, pp 706–718

9. Ammar Hammad Ali ,”Design of Secure Chatting Application with End to End Encryption for Android Platform”, Iraqi Journal for Computers and Informatics 43(1):6. June 2017.

10. Abdalbasit Mohammed Qadir; Nurhayat Varol,” A Review Paper on Cryptography”, International Symposium on Digital Forensics and Security