Honey Cipher Structure

M.Rambabu
M.Tech, Associate professor
Department of Computer Science and Engineering
K G Reddy College of Engineering and Technology, Moinabad, RR District, Telangana

Dr. M.V.Siva Prasad
B.E. M.Tech., Ph.D., MISTE, Principal
Department of Computer Science and Engineering
Anurag Engineering College, Kodada,suryapet,Telangana

Dr. Madhusoodanan Nair. M
M.Tech., Ph.D., LMISTE, Director
Department of Computer Science and Engineering
K G Reddy College of Engineering and Technology, Moinabad, RR District, Telangana

Abstract:- Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit. However, in today's computer-centric world, cryptography is most often associated with scrambling plaintext. Honey Cipher Structure is one of such secured techniques in cryptography. There are many structures available in security, Honey Cipher structure is new model in to provide security for plaintext of alphabets as well as numeric's. I planned to implement, this structure with eight levels first level contains eight elements, from first level to last level one element is decreased, and the last level contains only one element. In this honey cipher structure first level filled by the password and repeated characters are omitted in the password, password may also contains numeric's. After filling the password remaining levels are filled by the rest of the characters. This is reason sender can have the confident that the transferred message have secured. Honey structure is created by filling all characters and numeric's, next step honey form is converted into Honey cipher Structure. This structure represents the three digits of numbers, this form is called as honey cipher structure, and this can be protected the message. But to provide more security, this three digit numbers are considered as ASCII decimal values. The three numbered text is converted into ASCII characters, these characters are to be considered as a cipher text. This cipher text is transferred to receiver. Receiver decrypts this cipher text in reverse order to read the original message.

KEYWORDS: - Honey Structure, Honey Cipher Structure, ASCII Values, ASCII Character Representation.

I. INTRODUCTION

Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit. However, in today's computer-centric world, cryptography is most often associated with scrambling plaintext. Honey Cipher Structure is one of the secured techniques in cryptography. This is the new technique in the cryptography; the technique is converting the plain text into cipher text. Some of the techniques convert only characters, but this structure converts numeric's (0,1,2,3,4,5,6,7,8,9) along with the alphabets. The creation of the password includes mixed texts. This created password is filled in the first row of the honey form, the repeated characters are omitted and fill next character in the password, and after filling the password uncovered characters are filled in the rest of the levels [2]. Do the same process for numerics also. After reaching the last level. Generated expression is convert this honey form into honey cipher structure. This structure is associated with Ascii Table. In this Ascii Table Ascii values are converted into Ascii Characters. These Ascii Characters are known as cipher text [7].

Problem:-

There are many structures available in security, ours is a new model to provide security for the alphabets as well as numeric's. In this problem, structure contains eight levels, from first level to last level one element is decreased at each level and last level contains only one element. In this structure first level is filled by the password, the repeated characters in the password is omitted, password may contain numerics also. Same way rest of the alphabet characters starting from the first alphabet 'a" to z omitting the repeated alphabets are filled in remaining levels, this structure may contain numbers also, to produce the high security.

- *Existing System:-*

The existing system is pyramidal cipher. In this structure cipher text size is larger than plaintext. This structure has single conversion from plain text to cipher text using method. Opponent can easily break the cipher text with multiple attempts.

- *Proposed System:-*

In this problem I have converted plaintext in three ways, honey structure to cipher structure and this cipher text contain values this values are converted into character representation. I planned to print the cipher from character depending on precedence, because character contain two digit text, from these two I applied precedence.

II. LITERATURE SURVEY

Now a day's security is most popular in internet world, from a long time, Fiestal cipher structure, Ceaser cipher structure, DES, AES, etc,. methods are used to protect the information [1]. Pyramidal form is also one of the techniques in cryptography, in this model we can convert only alphabets, numerics are transferred in the same way. Attacker can capture and come to know that, displayed text may be original, like, phone numbers, home Address, something true. Except character conversion remaining all the text is not converted into the cipher text. Once a person's physical safety needs are relatively satisfied, the safety needs take precedence and dominate behavior. In the absence of physical safety – due to war, natural disaster, family violence, childhood abuse, etc. – people may experience post-traumatic stress disorder or transgenerational trauma. In the absence of economic safety (money count also not encrypted) [3]– due to economic crisis and lack of work opportunities – these safety needs manifest themselves in ways such as a preference for job security, grievance procedures for protecting the individual from unilateral authority, savings accounts, insurance policies, disability accommodations, etc.

III. THE PROPOSED SYSTEM

Honey Structure:-

These honey cipher can reveal the apparent address of the abuse and provide bulk spam capture (which enables operators to determine spammers' response mechanisms). For open relay honey cipher, it is possible to determine the e-mail addresses ("drop boxes") spammers' use as targets for their test messages, which are the tools they use to detect open relays. It is then simple to deceive the spammer: transmit any illicit relay e-mail received addressed to that drop box e-mail address. That tells the spammer the honey cipher is a genuine abusable open relay, and they often respond by sending large quantities of relay spam to that honey cipher which stops it. The apparent source may be another abused system—spammers and other abusers may use a chain of abused systems to make detection of the original starting point of the abuse traffic difficult.

This in itself is indicative of the power of honey cipher as anti-spam tools. In the early days of anti-spam honey cipher, spammers, with little concern for hiding their location, felt safe testing for vulnerabilities and sending spam directly from their own systems [5]. Honey cipher made the abuse riskier and more difficult. Spam still flows

through open relays, while most spam originates in the spammers hop through open relays across political boundaries to mask their origin. Honey cipher operators may use intercepted relay tests to recognize and thwart attempts to relay spam through their honey cipher. "Thwart" may mean "accept the relay spam but decline to deliver it." honey cipher operators may discover other details concerning the spam and the spammer by examining the captured spam messages.

In modern removable frame hives the nursery area is in the brood chamber, which beekeepers prefer to be in the bottom box. In the late winter and early spring as the brood cycle begins, the queen starts to lay eggs within the winter cluster in proximity to available honey stores. Honey bees tend to greatly expand the brood chamber as the season progresses. The relative location of the brood chamber within the beehive may also change as bee keepers add more boxes or as wild bees build fresh comb into available cavities. Some beekeepers ensure that the queen will not go into the upper boxes (called supers or honey supers) by placing a screen called a queen excluder between the boxes. The screen has precisely measured open spaces through which a worker bee can pass, but not a queen. Some beekeepers do not use excluders, but try to keep the queen within the intended brood area by keeping a honey barrier of capped honey, which the queen is reluctant to cross, above the brood. In feral hives the honey bees tend to put the brood at bottom center of the cavity, and honey to the sides and above the brood, so beekeepers are trying to follow the natural tendency of the bees.

In the mid to late spring, just before a bee hive would naturally split by swarming, beekeepers often remove frames of brood, with adhering bees, to make up new starter hives, called "nucs" or nucleus colonies. In areas where the climate is mild, one frame may be sufficient to start a new colony, with an added queen. But usually two to three frames are used, together with a frame that is predominantly honey. This ensures that there will be enough adult bees to provide the brood the adequate temperature and sufficient feed if there are a few rainy days when bees cannot gather nectar. If there are not enough adult bees to warm the combs, the brood may die from cold temperature overnight (aptly called "chilled brood").

- *OBJECTIVES*

 To gain new understanding of cryptographic models and techniques, in order to face current and future security challenges.
 To consolidate and strengthen the scientific excellence of cryptography using honey cipher
 It is not possible to hacking, it is multi way translation to convert the security
 Cryptography security system is to protect information resources at less cost than the value of the information that is being protected.
 Determining acceptable costs involves weighing the cost of the security versus the benefits of the security.

- *METHODOLOGY*

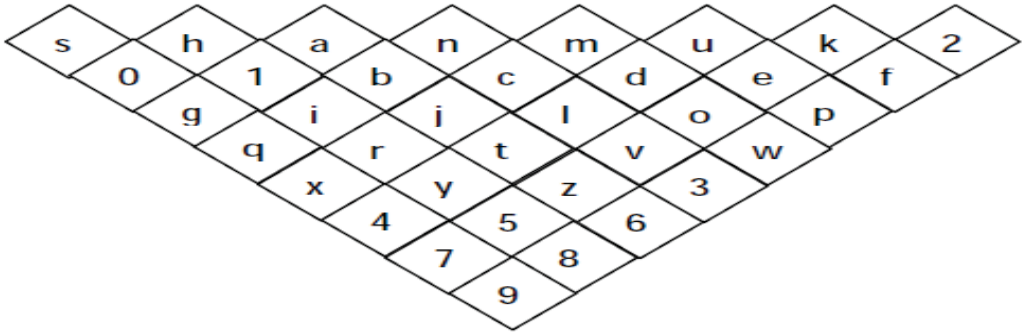
When we create the honey structured form, and convert into honey cipher structure. This Cipher structure follows the two digits number this is called as honey cipher structure. This cipher structure values are consider as ASCII decimal values, this ASCII values are converted into character representation. this character form also contain two digits but cipher form prints only one charter, this way we can produce the full cipher structure, which is send to receiver. Receiver deciphers this in reverse order to get plain text, which is send by sender.

IV. IMPLEMENTATION

This is the new technique in the cryptography; the technique is converting the plain text into cipher text. Some of the techniques convert only characters, but this structure converts numeric's (0,1,2,3,4,5,6,7,8,9) along with the alphabets. The creation of the password includes mixed texts. This created password is filled in the first row of the honey form, the repeated characters are omitted and fill next character in the password, and after filling the password uncovered characters are filled in the rest of the levels. Do the same process for numerics also. After

reaching the last level. Generated expression is convert this honey form into honey cipher structure. This structure is associated with Ascii Table in this Ascii table Ascii values are convert into Ascii Characters. These Ascii Character symbols are known as cipher text.

Honey Structure:-

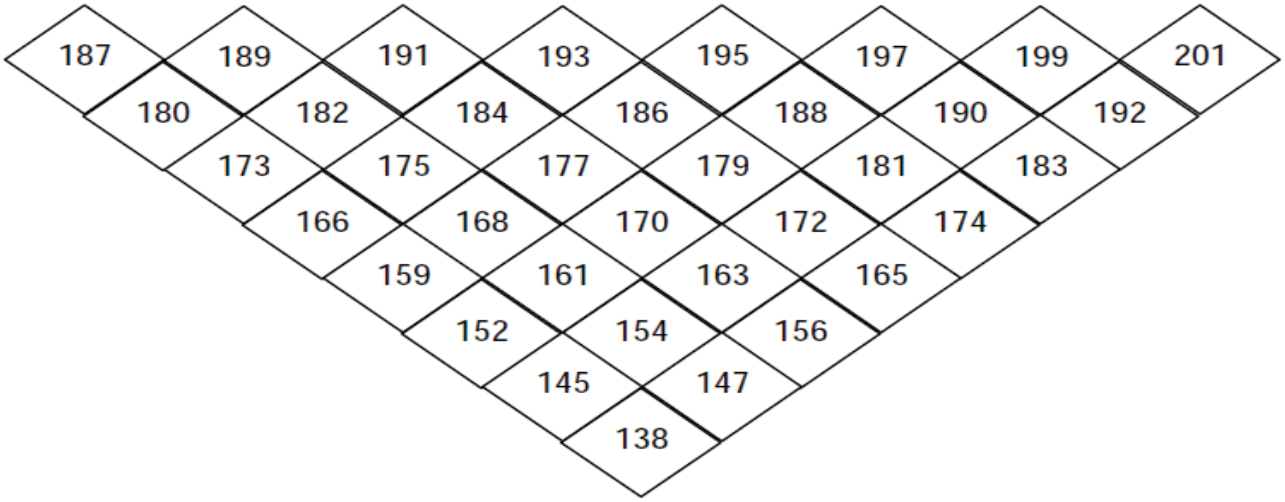


In this paper, I created the password,"Shanmukh2010", here h and 0 are repeated twice, the repeated characters in this password are omitted and follows the next characters [2]. Finally the filled password in this honey structure is "shanmuk201". This password is filled in the first level, and follows second level if not sufficient in the first level. After filling the password, remaining levels filled by the remaining characters. Finally fill the numeric's also to provide the security for home address. Whenever we create the structure, this structure specifies the all characters and numeric's. I planned to convert this structure in decimal numbers by creating the honey equation. Implementation of the honey cipher structure it contains eight levels, each level represents with elements. The structure of first level indicates eight elements, second level indicates seven elements, sixth level indicates six elements, and so on. From first level to last level one element is decreased at each level. The levels are represented with "i" and elements are represented with "j", this structure is mapping with the ASCII table, the importance of mapping with this table is that hexadecimal values are converted into character symbols. These character symbols are known as cipher text, this cipher text is considered as honey cipher text which is sent to receiver. This cipher is protected message. This is my paper to convert original message into cipher text in easiestt method. Generated equation for the honey structure into honey cipher structure is here $H_{i,j}$, the levels and elements of honey structure respectively,

$$H_{i,j} = 192+2*j-7*i;$$

This formula is created for convert the honey structure into honey cipher structure[7], and create the three digit number this is first stage of security but it contain three bit text for each honey character. In security bit cipher is the better for perfect security [1]. All the levels and all the elements in honey cipher structure are three digits number only, because two digits number are associated with the ASCII table some of the elements are specified two character symbols. But in cipher structure are bit cipher or stream cipher. This paper implemented in bit cipher, so each honey structure characters are must print only one bit cipher character. In ASCII three digits of decimal values are only associated with the one bit of cipher character symbols.

Honey Cipher Structure:-



Generate cipher text from character, depending on precedence; because character contains two digit texts, from these two I was applied precedence technique to print the one bit from the character. This is generating the plaintext and cipher text in same size.

ASCII Table and Description

ASCII stands for American Standard Code for Information Interchange. Computers can only understand numbers, so an ASCII code is the numerical representation of a character such as 'a' or '@' or an action of some sort. ASCII was developed a long time ago and now the non-printing characters are rarely used for their original purpose. Below is the ASCII character table and this includes descriptions of the first 32 non-printing characters. ASCII was actually designed for use with teletypes and so the descriptions are somewhat obscure. If someone says they want your CV however in ASCII format, all this means is they want 'plain' text with no formatting such as tabs, bold or underscoring - the raw format that any computer can understand. This is usually so they can easily import the file into their own applications without issues. Notepad.exe creates ASCII text, or in MS Word you can save a file as 'text only'. I adapted this information from a web site and I have made it available locally. Java actually uses Unicode, which includes ASCII and other characters from languages around the world[8]. ASCII Table specifies that following as an example. To converting as follows:-

Dec = Decimal Value

Char = Character

'5' has the int value 53

if we write '5'-'0' it evaluates to 53-48, or the int 5 and also if we write char c = 'B'+32; then c stores 'b'

The following conversion table is provided as a reference for ASCII and EBCDIC translation. When moving information (files or data buffers) between EBCDIC machines and ASCII machines it is quite often necessary to convert the information. If the data strings contain only display or printable characters then it is a straightforward, byte-for-byte conversion. However, in the real world the actual conversion of data strings between the ASCII and EBCDIC[7] encoding schemas is usually more complicated than a simple byte-for-byte conversion. For example, if the data strings contain packed or binary data or control information then the data conversion becomes content sensitive. The translation of records or data strings within a file may be an explicitly defined task

or it may be done as part of a file transfer process when files are being moved between systems that use different encoding schemas. If a data conversion is done by the file transfer process the data should be reviewed to ensure that special characters (currency symbols, the copyright symbol, the trademark symbol and more) are correctly converted. I have made a significant effort to ensure the documents and software technologies are correct and accurate. We reserve the right to make changes without notice at any time. The function delivered in this version is based upon the enhancement requests from a specific group of users. The intent is to provide changes as the need arises and in a timeframe that is dependent upon the availability of resources.

Bee brood frames are composed of brood at various stages of development - eggs, larvae, and pupae. In each cell of honeycomb, the queen lays an egg, gluing it to the bottom of the cell. The queen tends to lay brood in a circular or oval pattern. At the height of the brood laying season, the queen may lay so many eggs per day, which the brood on a particular frame may be virtually of the same age.As the egg hatches; worker bees add royal jelly - a secretion from glands on the heads of young bees. For three days the young larvae are fed royal jelly, then they are fed nectar or diluted honey.

Dec	Hx	Oct	Char	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
0	0	000	NUL (null)	32	20	040		Space	64	40	100	@	@	96	60	140	`	`
1	1	001	SOH (start of heading)	33	21	041	!	!	65	41	101	A	A	97	61	141	a	a
2	2	002	STX (start of text)	34	22	042	"	"	66	42	102	B	B	98	62	142	b	b
3	3	003	ETX (end of text)	35	23	043	#	#	67	43	103	C	C	99	63	143	c	c
4	4	004	EOT (end of transmission)	36	24	044	$	$	68	44	104	D	D	100	64	144	d	d
5	5	005	ENQ (enquiry)	37	25	045	%	%	69	45	105	E	E	101	65	145	e	e
6	6	006	ACK (acknowledge)	38	26	046	&	&	70	46	106	F	F	102	66	146	f	f
7	7	007	BEL (bell)	39	27	047	'	'	71	47	107	G	G	103	67	147	g	g
8	8	010	BS (backspace)	40	28	050	(	(	72	48	110	H	H	104	68	150	h	h
9	9	011	TAB (horizontal tab)	41	29	051	)	)	73	49	111	I	I	105	69	151	i	i
10	A	012	LF (NL line feed, new line)	42	2A	052	*	*	74	4A	112	J	J	106	6A	152	j	j
11	B	013	VT (vertical tab)	43	2B	053	+	+	75	4B	113	K	K	107	6B	153	k	k
12	C	014	FF (NP form feed, new page)	44	2C	054	,	,	76	4C	114	L	L	108	6C	154	l	l
13	D	015	CR (carriage return)	45	2D	055	-	-	77	4D	115	M	M	109	6D	155	m	m
14	E	016	SO (shift out)	46	2E	056	.	.	78	4E	116	N	N	110	6E	156	n	n
15	F	017	SI (shift in)	47	2F	057	/	/	79	4F	117	O	O	111	6F	157	o	o
16	10	020	DLE (data link escape)	48	30	060	0	0	80	50	120	P	P	112	70	160	p	p
17	11	021	DC1 (device control 1)	49	31	061	1	1	81	51	121	Q	Q	113	71	161	q	q
18	12	022	DC2 (device control 2)	50	32	062	2	2	82	52	122	R	R	114	72	162	r	r
19	13	023	DC3 (device control 3)	51	33	063	3	3	83	53	123	S	S	115	73	163	s	s
20	14	024	DC4 (device control 4)	52	34	064	4	4	84	54	124	T	T	116	74	164	t	t
21	15	025	NAK (negative acknowledge)	53	35	065	5	5	85	55	125	U	U	117	75	165	u	u
22	16	026	SYN (synchronous idle)	54	36	066	6	6	86	56	126	V	V	118	76	166	v	v
23	17	027	ETB (end of trans. block)	55	37	067	7	7	87	57	127	W	W	119	77	167	w	w
24	18	030	CAN (cancel)	56	38	070	8	8	88	58	130	X	X	120	78	170	x	x
25	19	031	EM (end of medium)	57	39	071	9	9	89	59	131	Y	Y	121	79	171	y	y
26	1A	032	SUB (substitute)	58	3A	072	:	:	90	5A	132	Z	Z	122	7A	172	z	z
27	1B	033	ESC (escape)	59	3B	073	;	;	91	5B	133	[	[	123	7B	173	{	{
28	1C	034	FS (file separator)	60	3C	074	<	<	92	5C	134	\	\	124	7C	174			|
29	1D	035	GS (group separator)	61	3D	075	=	=	93	5D	135	]	]	125	7D	175	}	}
30	1E	036	RS (record separator)	62	3E	076	>	>	94	5E	136	^	^	126	7E	176	~	~
31	1F	037	US (unit separator)	63	3F	077	?	?	95	5F	137	_	_	127	7F	177	&#127;	DEL

128	Ç	144	É	160	á	176	▒	192	└	208	╨	224	α	240	≡
129	ü	145	æ	161	í	177	▒	193	┴	209	╤	225	ß	241	±
130	é	146	Æ	162	ó	178	▓	194	┬	210	╥	226	Γ	242	≥
131	â	147	ô	163	ú	179	│	195	├	211	╙	227	π	243	≤
132	ä	148	ö	164	ñ	180	┤	196	─	212	╘	228	Σ	244	⌠
133	à	149	ò	165	Ñ	181	╡	197	┼	213	╒	229	σ	245	⌡
134	å	150	û	166	ª	182	╢	198	╞	214	╓	230	µ	246	÷
135	ç	151	ù	167	º	183	╖	199	╟	215	╫	231	τ	247	≈
136	ê	152	ÿ	168	¿	184	╕	200	╚	216	╪	232	Φ	248	°
137	ë	153	Ö	169	⌐	185	╣	201	╔	217	┘	233	Θ	249	∙
138	è	154	Ü	170	¬	186	║	202	╩	218	┌	234	Ω	250	·
139	ï	155	¢	171	½	187	╗	203	╦	219	█	235	δ	251	√
140	î	156	£	172	¼	188	╝	204	╠	220	▄	236	∞	252	ⁿ
141	ì	157	¥	173	¡	189	╜	205	═	221	▌	237	φ	253	²
142	Ä	158	₧	174	«	190	╛	206	╬	222	▐	238	ε	254	■
143	Å	159	ƒ	175	»	191	┐	207	╧	223	▀	239	∩	255	

The purpose of this document is to provide a quick reference for ASCII translation [8]. This document may be used as a tutorial for new programmers or as a quick reference for experienced programmers. In the world of programming there are many ways to solve a problem. This document and the links to other documents are intended to provide a greater awareness of the Data Management and Application Processing alternatives. The documentation and software were developed and tested on systems that are configured for an environment based on the hardware, operating systems, user requirements and security requirements. Therefore, adjustments may be needed to execute the jobs and programs when transferred to a system of a different architecture or configuration. Services have experience in moving or sharing data or application processing across a variety of systems. Preparing the application programs will require the transfer of source members that will be compiled and deployed on the target platform. The data will need to be transferred between the systems and may need to be converted and validated at various stages within the process. Has the technology, services and experience to assist in the application and data management tasks involved with doing business in a multi-system environment.

V. CONCLUSION

This paper is present conversation from ASCII values to ASCII character symbols, these character symbols are knon as cipher text in this paper. Decryption is very easy to reconvert cipher text to plain text. But conversation is very intresting it may provide security, and there is a possibilty to capture and guess the cipher text to plain text by multiple pacticess. I thik other than ASCII, if this honey cipher strucutre is associated with any another algorithms in security, an opponent can not be guess the plain tect. If we create any secure table in database with more complicate and tuff guessing. So we can protect plaintexy from opponent and can transfer messages with confidential.

VI. ACKNOLEDGEMENT

I authored this paper on secuirty transfer meaasges, with the support of my external guide, Dr.M.V.SIVA PRASAD, B.E.,M.Tech.,Ph.D.,MISTE, Principal, Anurag Engineering College, KDD. I am thankful to my chairman, K..Krishna Reddy garu for his support and Director Dr. Madhusoodanan Nair. M for his guidance and inputs. Finally I am indebted to my family members for providing a peaceful environment, to create this Honey Cipher structure.

REFERENCES

[1] Network Security Essentials by "William Stalling", Third Edition.
[2] Security using Pyramidal Cipher Form from IJFTE Journals.
[3] W. Ehrsam, etal., " A Cryptography Key Management Scheme for Implementing the Data Encryption Standard", IBM System Journal,VOL.7,PP.-125,2010.
[4] J. Katz and Y. Lindell, Introduction to Modern Cryptography;,Chapman & all/CRC.2008.
[5] T.Fukunga and J. Takahashi, "Practical fault attack on a Cryptographic LSI with ISO/IEC 18033-3 Block Ciphers", 2010.PP.84-92.
[6] A. Barenghi, etal., " Low Voltage fault attacks to AES and RSA on general purpose processors", IACR Eprint archive, Vol.130,2010.
[7] ASCII or EBCDIC, Translation Tables from Google Wikipedia.
[8] http://www.malighting.com, for conversation from ASCII Decimal Values to Character Symbols.