PDPKDES
(Pre Distributed Powerful Key for Data Encryption Standard)

Prerna Mittal
Computer Science & Engineering
B.S Anangpuria Institute of Technology and Management
Faridabad, India
Prerna.it.mittal@gmail.com

Bhawna Chauhan
Computer Science & Engineering
B.S Anangpuria Institute of Technology and Management
Faridabad, India
Chauhan.bhawna@gmail.com

***Abstract*—Data encryption standard in spite of being a great algorithm in terms of a good combination of confusion and diffusion steps, doesn't largely used because of a weak key concept. The key used in DES is only 64 bits (or 56 bits) long. This paper introduces a concept of pre distributed powerful key for DES. In this for every round of DES a new key is getting used which makes cryptanalyst to attack not 56 bits but 16 keys of 56 bits each which makes it a much stronger algorithm.**

Index Terms- Encryption algorithms, Data encryption standard, Key pool, Pre distributed keys, Weak key, Powerful key, Key pool.

I. INTRODUCTION

Every encryption algorithm has two basic criteria's for a good algorithm. One is encryption steps and second is length of key. There are various algorithms available like:

DES (Data Encryption Standard): It was the first encryption standard to be recommended by NIST (National Institute of Standards and Technology)[2]. It became a standard in 1974. Since that time, many attacks and methods recorded that exploit weaknesses of DES, which made it an insecure block cipher because of smaller key length.

3DES (Triple DES): Because of the smaller key [3] brute force attack was much simpler in DES. It is an enhancement to DES as the key is multiplied 3 times and make it a stronger encryption algorithm. However, it is slower than other block cipher methods.

AES (Advanced Encryption Standard): To avoid the above issues AES was recommended by NIST to replace DES. . It has 3 different key sizes: 128, 192 and 256 bits used for the encryption of the 128 bit block size data. It includes three different default rounds depending upon the key length i.e. 10 for a 128 bit key size, 12 for a 192 bit key size and 14 for a 256 bit key size. The design of sub key has been designed by considering the side channel and cache timing based attacks [4].

Blowfish: It is a freely available symmetric block cipher designed in 1993 by Bruce Schneier. It includes key dependent S boxes and a highly complex key schedule which produces overheads. It has a 64 bit block size and a variable key length from 1 to 448 bits. The technique uses the concept of sub keys; these are generated by the algorithm itself. It is a very fast approach for encrypting the data with same keys. When keys are changed then new key under goes from pre-processing operation which consumes more time [4].

An algorithms' key length is a very critical measure for the weakness or strength of an algorithm. DES is a good algorithm [8] but has the biggest weakness of small key length which makes data insecure due to easy brute force attacks.

Algorithm used for DES is:

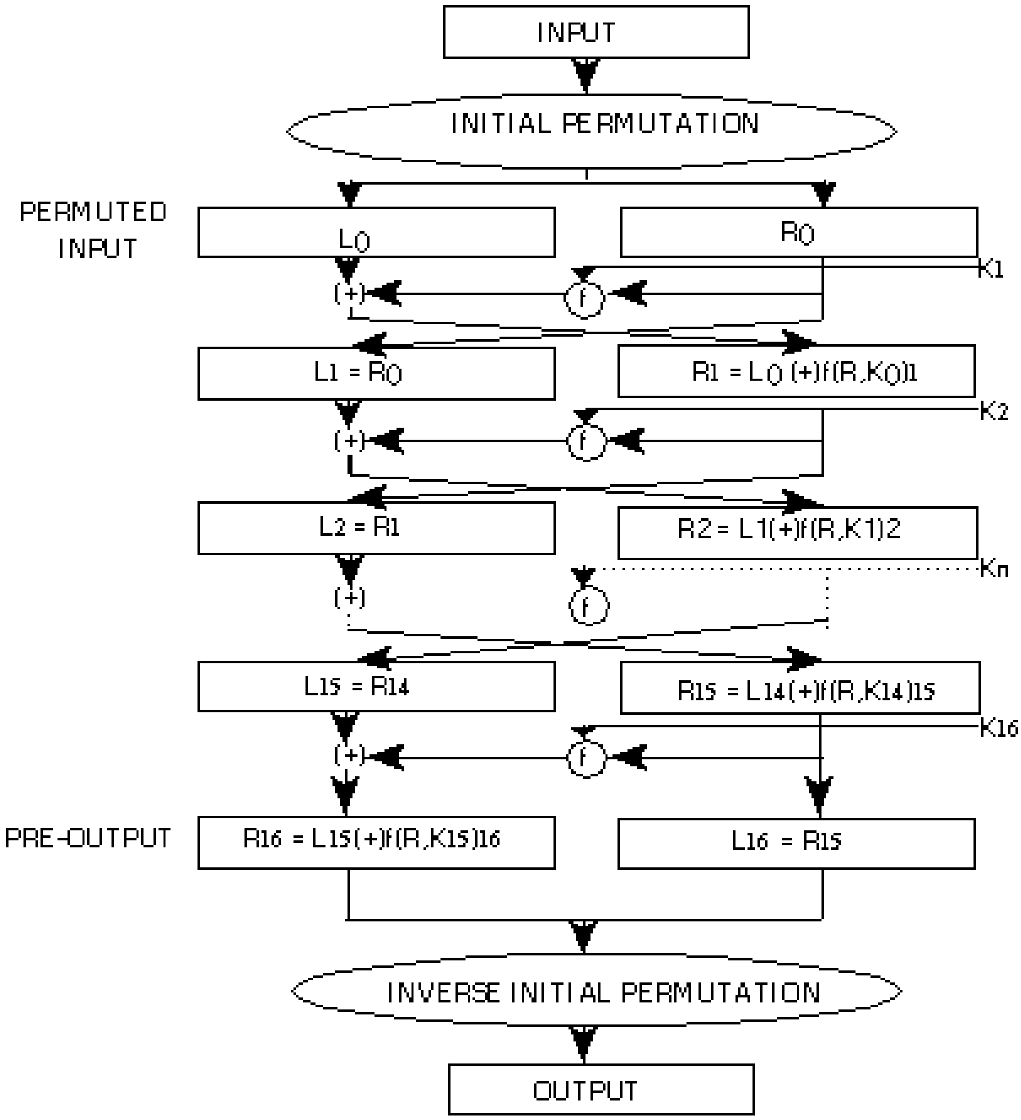

Fig 1: DES encryption algorithm

II. PRE DISTRIBUTION OF KEY

A. Sending a file

First, a file is shared between the two users or the sender and the receiver among which the communication needs to take place. This pre distributed file is converted into bytes. And these bytes work as a key pool. Any byte can be chosen as the starting point of the key.

When we sent a key on the network, security of key is equally important. Thus in actual implementation we sent the secured key like PGP [11], and for this kind of security we use RSA[10].

One file of 1.88 Kb is decrypted and converted into 1933 bytes[5].

255 216 255 224 0 16 74 70 73 70 0 1 1 0 0 1 0 1 0 0 255 219 0 67 0 9 6 7 8 7 6 9 8 7 8 10 10 9 11 13 22 15 1312 12 13 27 20 21 16 22 32 29 34 34 32 29 31 31 36 40 52 44 36 38 49 39 31 31 45 61 45 49 53 55 58 58 58 35 43 63 68 63 56 67 52 57 58 55 255 219 0 67 1 10 10 10 13 12 13 26 15 15 26 55 37 31 37 55 55 55 55 55 55 5555 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 5555 55 55 55 55 55 55 255 192 0 17 8 0 80 0 80 3 1 34 0 2 17 1 3 17 1 255 196 0 28 0 0 1 5 1 1 1 0 0 0 0 0 0 0 0 0 0 7 1 4 5 6 8 3 2 0 255 196 0 63 16 0 2 1 3 1 5 5 3 9 4 11 0 0 0 0 0 1 2 3 0 4 17 33 5 6 18 49 65 7 19 20 81 113 34 97 145 35 50 66 84 129 147 177 209 240 52 161 178 193 21 22 36 67 82 99 100 114 116 132 241 255

196 0 26 1 0 2 3 1 1 0 0 0 0 0 0 0 0 0 0 0 4 5 2 3 6 1 0 255 196 0 39 17 0 1 4 1 3 2 6 3 0 0 0 0 0 0 0 0 1 0 2 3 17
4 5 18 33 49 65 19 34 50 51 81 129 20 97 113 255 218 0 12 3 1 0 2 17 3 17 0 63 0 56 214 120 237 246 121 99
223 88 68 114 200 131 192 199 243 92 129 243 158 180 61 103 94 223 215 59 237 9 255 0 65 31 241 61 29
167 11 158 128 81 127 68 57 241 87 63 88 155 239 15 231 95 120 171 159 172 77 247 134 184 170 48 58 157
43 160 67 90 40 225 46 28 182 149 36 210 245 226 174 62 177 55 222 31 206 147 197 92 227 246 137 190 240
254 117 247 116 105 12 100 30 120 169 187 20 158 129 123 114 67 117 114 79 237 19 105 254 97 252 233
124 85 207 214 38 251 195 92 184 74 200 65 228 122 215 190 1 231 65 71 0 125 154 231 162 149 162 63 96
179 77 38 253 50 201 44 140 60 28 186 51 147 213 43 70 10 2 246 9 178 94 61 187 38 211 155 137 67 193 36
112 140 124 237 87 136 254 189 244 122 20 143 49 155 37 175 210 155 8 33 45 103 158 223 23 59 237 6 132
255 0 97 143 151 251 158 180 53 5 251 85 216 210 109 109 249 128 32 246 69 156 97 142 57 123 79 87 105
142 107 103 220 227 64 2 185 45 237 225 6 94 34 160 48 13 161 198 10 154 145 180 217 242 220 168 104 163
44 124 128 162 150 211 178 217 187 183 178 225 149 118 60 87 173 175 123 222 2 218 99 67 143 95 221 93
236 247 199 101 45 178 54 206 134 59 117 111 238 149 0 42 124 180 231 235 255 0 148 91 245 182 179 150
54 194 155 112 158 243 181 198 138 21 79 179 102 131 73 98 100 62 68 83 73 173 248 84 158 163 90 44 79
117 14 244 197 58 74 87 141 24 136 91 168 211 31 188 230 168 59 107 100 247 83 196 138 195 137 100 225
101 229 77 52 252 230 102 198 104 83 135 100 30 76 79 198 148 53 199 131 208 170 236 150 228 54 0 233
154 145 221 205 136 251 82 231 229 51 29 172 35 138 121 122 42 254 191 153 169 123 93 133 227 174 64
141 248 97 80 76 146 190 129 7 175 216 106 211 21 165 189 157 170 65 12 4 194 164 180 80 157 26 102 207
207 126 170 49 131 174 154 12 244 21 116 212 215 87 117 64 200 177 194 179 118 114 168 55 134 19 195
220 197 225 100 91 88 70 152 81 195 150 62 254 88 242 24 234 77 21 5 11 123 58 225 27 207 33 108 205 114
214 239 223 204 49 194 154 140 32 61 124 252 249 150 215 20 82 21 153 212 125 255 0 164 110 63 161 45 82
119 189 145 54 202 18 6 76 43 147 212 128 77 93 170 143 190 166 47 233 68 12 73 126 228 96 15 83 75 37 62
84 100 62 165 23 123 197 115 106 194 52 239 27 160 199 51 84 41 183 35 107 222 109 25 228 182 183 75 88
164 110 32 211 72 2 235 230 6 191 1 87 25 47 218 60 1 194 0 232 9 207 219 154 75 173 186 176 219 22 145
130 244 201 243 161 218 72 54 10 56 242 40 133 15 6 230 220 108 144 46 33 218 209 203 42 158 38 136 161
0 158 190 209 36 252 69 38 208 217 171 180 110 209 166 246 37 67 242 168 163 218 102 198 52 252 249 83 9
183 168 207 112 240 42 77 197 243 65 211 173 57 183 187 218 22 151 205 45 229 183 127 97 117 194 89 225
82 100 132 96 12 178 131 151 65 141 125 115 167 42 97 166 72 248 231 222 195 95 40 29 78 142 62 199 14
123 39 137 20 112 160 88 251 180 142 46 92 71 228 212 243 203 31 166 220 180 228 63 125 55 147 11 8 99
36 177 44 135 5 216 124 188 164 116 81 205 64 39 24 26 227 144 28 234 94 226 217 225 153 25 138 174 85
90 39 118 86 108 105 170 34 147 141 49 140 212 100 171 221 6 149 138 219 6 207 121 36 196 52 154 105 133
28 177 248 127 134 180 205 126 238 109 102 216 72 52 172 123 128 10 109 244 70 17 219 70 45 228 238 109
128 5 152 100 100 147 230 52 200 30 236 235 68 193 67 62 207 224 141 119 129 166 134 9 8 104 27 142 230
102 249 71 212 99 32 235 208 249 15 117 19 5 35 212 61 255 0 164 219 16 220 105 104 101 218 52 165 119
130 53 215 30 25 121 29 121 181 19 104 71 218 174 208 130 13 229 72 11 170 205 225 80 224 176 28 203 99
157 9 30 59 242 28 35 103 84 79 138 216 188 206 81 145 176 145 149 23 132 156 106 73 0 15 92 213 67 104
221 77 180 47 196 74 249 140 57 238 248 70 133 121 103 237 174 243 65 222 58 52 247 17 142 240 158 17
223 5 39 208 19 249 215 169 23 187 154 52 104 227 134 101 33 99 115 175 22 53 229 166 15 235 221 71 205
161 72 41 177 184 19 221 114 45 77 128 151 60 127 19 203 109 131 52 115 165 226 40 225 39 5 93 130 145
143 165 147 167 58 178 69 182 162 181 145 123 183 130 55 69 0 183 126 163 166 51 132 4 255 0 58 171 195
220 94 179 153 209 34 145 92 171 178 179 49 7 204 2 227 60 244 167 80 236 93 152 177 40 80 172 122 150
187 78 35 234 3 10 97 141 166 197 142 57 60 148 187 43 53 211 154 119 110 138 125 246 186 237 73 91 195
200 243 50 145 198 208 174 48 8 228 206 125 255 0 15 117 71 205 112 182 141 226 37 150 210 210 66 163
138 89 31 142 64 71 145 200 248 100 254 53 13 117 179 26 37 62 14 70 83 210 50 235 145 232 234 220 67
208 228 85 90 114 210 158 60 72 11 128 75 0 50 193 131 115 198 135 85 231 129 70 182 22 180 80 232 169
99 3 205 218 45 118 111 181 118 117 222 246 119 22 247 115 92 207 225 164 246 181 88 192 5 62 142 128 31
176 233 141 104 182 43 62 246 34 175 253 119 82 203 167 131 151 92 99 164 117 160 133 103 245 33 83 253
4 202 6 134 178 130 90 2 246 220 203 30 250 198 204 170 217 176 143 57 25 199 180 244 122 172 253 219
193 35 124 225 255 0 131 31 241 61 87 132 253 147 7 47 78 45 138 161 225 108 111 161 224 120 86 54 206
67 198 0 35 249 26 149 150 97 29 148 54 38 78 33 26 137 36 158 65 147 26 41 207 23 175 64 58 213 90 57 93
62 105 248 87 70 184 102 201 36 235 128 115 215 7 35 224 105 235 114 133 221 114 130 13 61 207 10 199
41103 146 89 217 13 187 48 86 120 211 65 31 68 66 0 246 164 111 45 48 43 148 153 12 82 105 155 10 112
193 46 20 99 166 188 36 254 31 10 130 55 47 156 171 176 60 76 195 94 76 71 63 94 153 164 107 150 42 136
52 69 30 202 116 21 47 204 160 187 180 39 75 5 173 171 180 150 143 41 98 49 237 144 113 240 166 172 11
103 95 100 15 215 235 223 241 228 239 158 164 159 121 175 37 155 161 170 142 89 82 229 17 187 18 152
182 251 132 215 2 202 92 100 242 213 43 64 14 117 158 123 12 24

B. Choose any key

The byte chosen are the highlighted ones. These can be used as the key pool

223 88 68 114 200 131 192 199 243 92 129 243 158 180 61 103 94 223 215 59 237 9 255 0 65 31 241 61 29 167 11 158 128 81 127 68 57 241 87 63 88 155 239 15 231 95 120 171 159 172 77 247 134 184 170 48 58 157 43 160 67 90 40 225 46 28 182 149 36 210 245 226 174 62 177 55 222 31 206 147 197 92 227 246 137 190 240 254 117 247 116 105 12 100 30 120 169 187 20 158 129 123 114 67 117 114 79 237 19 105 254 97 252 233 124 85 207 214 38 251 195 92 184 74 200 65 228 122

To take such a long key we have taken only the position byte .Thus:

- No overhead of sending the key over the network.
- Any number of keys can be chosen
- And if the file is never sent on the network. This cannot be cracked any time.

But since DES has a small key length, brute force can be applied on it and thus cryptanalysis is easily possible.

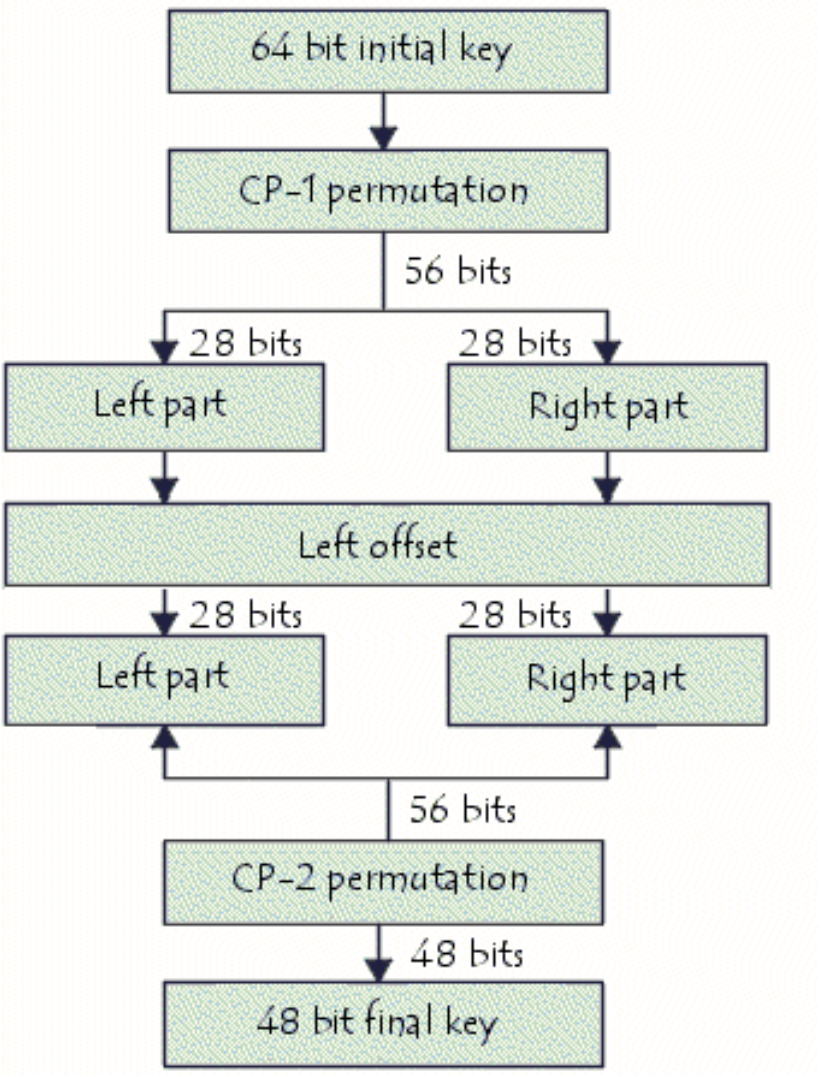

Figure 2 Actual key generation algorithm

III. PROPOSED IDEA OF POWERFUL KEY FOR DES

In this paper we introduce a concept which eliminates the weakness of 56 bit key of DES. DES goes under 16 rounds for the complete encryption. For every round sub key is generated from a single key. That means f the key is deduced, decryption of text becomes simpler. But if we give completely different key for every round of DES then cryptanalyst has to apply brute force attack on 16 56bit sized keys i.e. 16*56 combinations need to be applied. It means 2896 combinations need to be tried which makes it strongest of all algorithms.

When we choose a position then we can provide different keys for different rounds.

Round 1: 223 88 68 114 200 131 192 199

Round 2: 243 92 129 243 158 180 61 103

Round 3: 94 223 215 59 237 9 255 0

Round 4: 65 31 241 61 29 167 11 158

Round 5: 128 81 127 68 57 241 87 63

Round 6: 88 155 239 15 231 95 120 171

Round 7: 159 172 77 247 134 184 170 48

Round 8: 58 157 43 160 67 90 40 225

Round 9: 46 28 182 149 36 210 245 226

Round 10: 174 62 177 55 222 31 206 147

Round 11: 197 92 227 246 137 190 240 254

Round 12: 117 247 116 105 12 100 30 120

Round 13: 169 187 20 158 129 123 114 67

Round 14: 117 114 79 237 19 105 254 97

Round 15: 252 233 124 85 207 214 38 251

Round 16: 195 92 184 74 200 65 228 122

The only concept we need to remember at the time of decryption,

Round 16 key will be used for round 1 and

Round 15 key will be used for round 2 and so on and the process will be reversed.

In the DES actual key generation algorithm:

Step 1: we take one key.

Step2: It undergoes Permuted choice -1.It makes it 56 bit key.

Step3: Then the 56 bit key is divided into 2 halves.

Step4: Now these left part and right part undergoes left shifts which makes sub keys.

Step5: There are 16 sub keys generated for every round of algorithm.

Step6: Now these 56 bit sub keys undergoes PC-2(Permuted choice-2) .

Step7: And the resultant key generated is of 48 bits.

PDPKDES algorithm:

Step1: A file is converted into bytes.

Step2: A position is chosen to generate keys.

Step3: Now 64*16 /8 =128 bytes are chosen.

Step4: First 8 bytes are used for Round 1.

Step5: Next 8 bytes are used for Round 2 and so on.

Step6: 16 altogether different keys are generated.

Step7: Now this key undergoes PC-1 and 56 bit key is generated.

Step8: And then this key undergoes PC-2 and 48 resultant key is generated.

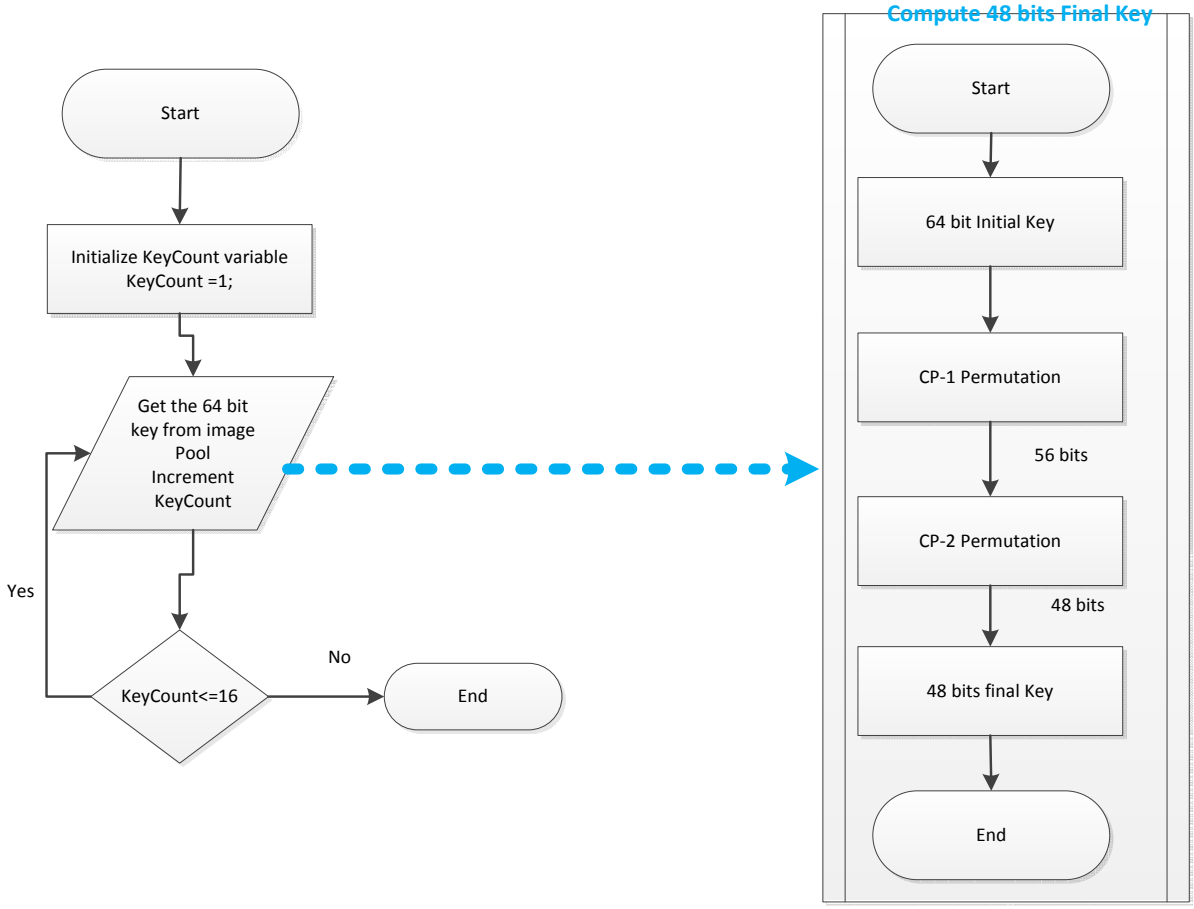

Fig 3: New key generation algorithm

IV. RESULTS

Data To Encrypt – Deepak		Cipher Data - ¥àÕ>\@5^
Cipher Data - ¥àÕ>\@5^		Decrypted Data - deepak

Round #	Key	Encrypted Data	Decrypted Data
Round 1	0 68 0 0 0 182 0 0	làüL§ ¥	¢»;mÒà
Round 2	0 0 0 0 0 0 0 0	L§ ¥üÑ	†Ýœv¢»;m
Round 3	0 59 9 0 0 252 17 0	üÑœ,‹ãÊ|	yÀòA†Ýœv
Round 4	0 32 69 77 70 0 0 1	‹ãÊ|q%<û	÷¬YyÀòA
Round 5	0 204 2 0 0 13 0 0	q%<û_dVs	1Ê…í÷¬Y
Round 6	0 2 0 0 0 0 0 0	_dVs²…T	$`èñ1Ê…í
Round 7	0 0 0 0 0 0 0 0	²…T #	É Š{$`èñ
Round 8	0 0 5 0 0 192 3 0	# ß U	ß U É Š{
Round 9	0 24 1 0 0 210 0 0	ß U É Š{	# ß U
Round 10	0 0 0 0 0 0 0 0	É Š{$`èñ	²…T #
Round 11	0 0 0 0 0 192 69 4	$`èñ1Ê…í	_dVs²…T
Round 12	0 80 52 3 0 70 0 0	1Ê…í÷¬Y	q%<û_dVs
Round 13	0 44 0 0 0 30 0 0	÷¬YyÀòA	‹ãÊ|q%<û
Round 14	0 86 0 105 0 115 0 105	yÀòA†Ýœv	üÑœ,‹ãÊ|
Round 15	0 111 0 32 0 77 0 101	†Ýœv¢»;m	L§ ¥üÑ
Round 16	0 116 0 97 0 102 0	¢»;mÒà	làüL§ ¥

Here note that Data after encryption Round 1 = Data before decryption Round 16= làüL§ ¥

Data after encryption Round 2 = Data before decryption Round 15= L§ ¥üÑ

And Data after encryption Round 16 =Data before decryption round 1 = ¢»;mÒà

Data after encryption Round N= Data before decryption Round 16-N.

V. CONCLUSION

This paper is on a new research topic about making already given algorithms stronger by giving them powerful keys for every round .By applying different key for every round we have made the cryptanalyst to break 2896 bits instead of 256 which takes years to try for. We can easily implement this concept in other algorithms such as AES, twofish, blowfish etc.

REFERENCES

[1] G. Eason, B. Noble, and I. N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. *(references)*

[2] Yashpal Mote, Paritosh Nehete, Shekhar Gaikwad ," Superior Security Data Encryption Algorithm(NTRU)", An International Journal of Engineering Sciences ISSN: 2229-6913 Issue July 2012, Vol. 6.

[3] https://www.princeton.edu/~achaney/tmve/wiki100k/docs/Key_size.html

[4] Ajay Kakkar, M. L. Singh, P.K. Bansal," Comparison of Various Encryption Algorithms and Techniques for Secured Data Communication in Multinode Network", International Journal of Engineering and Technology Volume 2 No. 1, January, 2012

[5] [13]Prerna Garg,Deepak Garg," Generation of a pool of variable size symmetric keys through Image", International Journal on Computer Science and Engineering (IJCSE), Vol. 3 No. 10 October 2011

[6] William Stallings "Cryptography and Network Security",3rd Edition, Prentice-Hall Inc., 2005.

[7] Diaa Salama Abd Elminaam1, Hatem Mohamed Abdual Kader2, and Mohiy Mohamed Hadhoud2," Performance Evaluation of Symmetric Encryption Algorithms on Power Consumption for Wireless Devices", International Journal of Computer Theory and Engineering, Vol. 1, No. 4, October, 2009 1793-8201

[8] Ayushi," A Symmetric Key Cryptographic Algorithm", 2010 International Journal of Computer Applications (0975 - 8887) Volume 1 – No. 15

[9] Hamdan.O.Alanazi, B.B.Zaidan, A.A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani," New Comparative Study Between DES, 3DES and AES within Nine Factors", JOURNAL OF COMPUTING, VOLUME 2, ISSUE 3, MARCH 2010, ISSN 2151-9617

[10] Dane Henry, RSA: Asymmetric Cryptography and Algorithm Analysis for a Secure Computing Environment, http://www.dwhenry.com/files/RSA.pdf

[11] Jessica J. Benz, "PGP: A Hybrid Solution",http://www.sans.org/reading_room/whitepapers/vpns/pgp-hybrid-solution_717

AUTHORS PROFILE

Ms. Prerna Mittal has a total experience of 8 years in the software industry and as a lecturer in an engineering college. She has explored the subject of network security and cryptography to a large extent. In her thesis also, she is working on the new concepts to avoid sending the key over and over again and make the best use of both symmetric and assymetric key algorithms.

Ms. Bhawna Chauhan has a total experience of 8 years as a lecturer in an engineering college and she is a very successful guide in encouraging students towards research and making them a powerful competitor in the industry and science research areas.