Generation of a pool of variable size symmetric keys through Image

Prerna Garg
B.S.A.I.T.M. Faridabad
Haryana, India
prerna.it.mittal@gmail.com

Deepak Garg
Senior Software engineer
Stryker Global Technology Center, Gurgaon,
Haryana, India
deepakgarg.garg@gmail.com

***Abstract*— This paper introduces a new concept of the generation of a unending pool of keys through an image leaving behind the idea of sending keys every time for encryption and decryption. This can help in avoiding the problem of frequent key exchanges and the after affects associated with it. In this a single image is used to generate the various keys. Thus say ,if the image is of 2n bytes, taking n from 0 to any valid integer value gives a big pool of keys making it useful for any symmetric encryption technique, DES, AES, RC4, CAST, twofish, blowfish etc. This adds the advantage of one time usage of key and avoids the disadvantage of securing and sending it on the network.**

Keywords - Key generation ; Image for key generation; Symmetric encryption;Assymetric encryption;Cryptography.

I. INTRODUCTION

In terms of network security, cryptography is a big concept. Till now, a lot of asymmetric and symmetric encryption techniques are suggested. Symmetric techniques[1][2] like DES, AES, CAST, 3DES and the asymmetric like RSA, Diffie- Hellman, knapsack and ECC[1][2][3][4]. But the problem of key hacking is always faced in symmetric algorithms and ease in complexity of algorithms in Asymmetric encryption. Thus to solve the issues, the symmetric encryption technique is used but the key chosen is locked with asymmetric key [1]. But this mechanism is generally one time usable and the transfer of big encrypted keys becomes an issue [1].Larger the key length, better the algorithm [7], is what has been observed in the study of cryptography or symmetric key algorithms

Thus to solve the problem, an algorithm is proposed which will solve the issue of transferring the encrypted symmetric key, only the asymmetric key can be used. As this is asymmetric key, problem of security is solved.

A. Advantages and Disadvantages of Symmetric algorithm:

Advantages [1]:

1. Encryption is secure if the key is not leaked out.
2. Encryption and data transmission is much faster than asymmetric one.
3. Symmetry of key allows encryption and decryption very easy.

Disadvantages [1]:

Security of key is very important as if the key is leaked then attacker can easily decrypt the data.

Solution:

1. Face-to-face key exchange is a solution but not feasible every time.

2. Keys should be changed frequently.
   - Keys should be changed frequently but is not possible in large groups.

- Distribution of keys becomes a problem, especially if keys change Frequently and all the keys must be encrypted individually before transfer.

B. *Advantages and Disadvantages of Asymmetric algorithm[1]:*

Advantages:

1. Key is a secret, never need to be transmitted so no chance of leaked out.
2. It helps mainly in digital signatures and authentication.

Disadvantages:

1. It is a much slower technique than private key cryptography.
2. Much larger keys are required to achieve the same level of security.
3. These are susceptible to impersonation attacks. Very few algorithms can be used for both encryption and key distribution.

Solution: Mainly used for key distribution

C. ***Proposed Solution:***

The solution is to combine both symmetric and asymmetric encryption algorithm. One example is PGP [5] in which symmetric key is encrypted with the help of asymmetric key and then the text is encrypted with symmetric key. This covered disadvantages of both public and private key cryptography but the problem of frequent key exchange and encryption of symmetric key is not solved through PGP. One such approach has been introduced in AES [6] and has proved to be very useful. Also a random pool of keys generation has been introduced for RSA [8].One more approached has been proposed [10] but that is not again applicable for every symmetric algorithm. The approaches above are for only fixed algorithms, a similar concept is now introduced in this algorithm which can be accepted by any algorithm or even a mix of algorithm at any time.

This idea is proposed and implemented with the concept of using image to convert into keys with the key value pairs as same image can be used many times to solve this problem.

II. IDEA PROPOSED AND IMPLEMENTED

A. Proposed Idea

Step1: First an encrypted image [9] is transferred. This is one time transfer i.e. this image will be used to generate various keys.

Step2: Decrypt it.

Step3: Convert image into bytes. This is also a onetime process saving a lot of resources and time but a onetime process each at the sender and receiver side.

Step4: Now, since this image will be transferred on network, it can be hacked. Thus to choose key bits within the image we take the help of public key encryption and thus an asymmetric key pair is chosen among the sender and receiver.

Step5: With the help of this key, we will choose bytes within the image and convert these bytes into bits. These bits are our symmetric key.

Step6: Now text will be encrypted using this key and encrypted text will be transferred.

Step7: At the receiver’s end, the encrypted text is decrypted with the bits generated from image using the asymmetric key pair.

III. ALGORITHMS

This section describes the complete procedure to explain how the Image is transferred. Algorithm of generation of key at both sender and receiver’s side

Step1: Image I is transferred

Step2: Convert image into bytes, say B [Length]

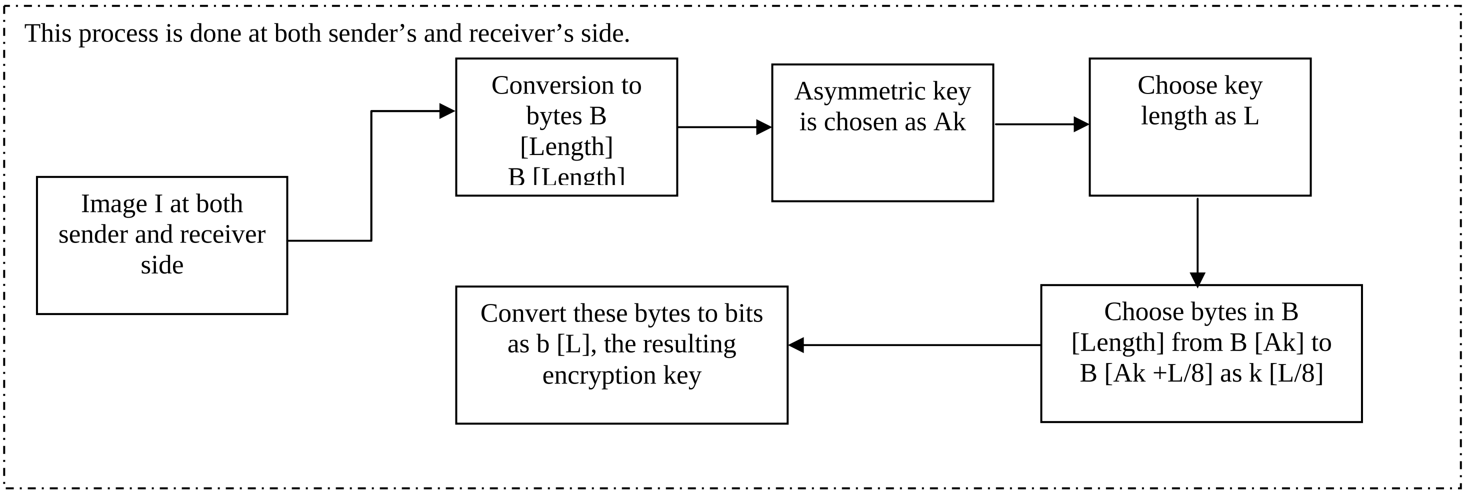
Step3: Choose asymmetric value Ak.

Step4: Choose key length L, anywhere from 8 bits to 2056 or more.

Step5: Now take out bytes from B [AK] to B [AK +L/8] as k [L/8].

Step6: Now convert these bytes to bits b [L].

Step7: This is the resulting key.

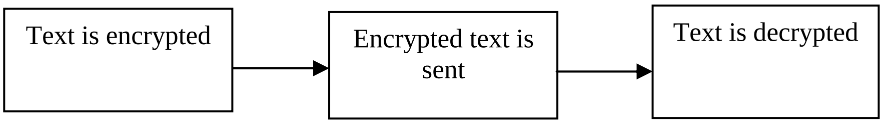

This process is done at both sender's and receiver's side.
Image I at both sender and receiver side
Conversion to bytes B [Length] B [Length]
Asymmetric key is chosen as Ak
Choose key length as L
Choose bytes in B [Length] from B [Ak] to B [Ak +L/8] as k [L/8]
Convert these bytes to bits as b [L], the resulting encryption key

B. Algorithm at receiever's side

Step1: Image is received.

Step2: b [L] is generated.

Step3: Using b [L] CT text is decrypted to make plaintext PT.



C. Image with example

One image of 1.88 Kb is decrypted and converted into 1933 bytes.

```
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 13
12 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 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 55 55 55
55 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 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 41
103 146 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 24 223 159 250 82 254 41 90 24 115 164 185 210 153
102 220 126 17 80 138 98 255 217
```

This byte conversion is required only once at both receiver’s and sender’s side

The keys can be generated from 1st till the last byte.

Taking from 128th bit for 256 length of key
The resultant key is
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 55 255 192

```
111011001110110011101100111011001110110011101100111011001110110011101100111011001110110011
101100111011001110110011101100111011001110110011101100111011001110110011101100111011001110
1100111011001110110011101100111011001110110011101100111011001111111100000011
```

Taking from 56th bit for 256 length of key
The resultant key is

```
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
101110001111100011111000001001000001010000101100001101000010010001100100100011001110010011
111000111110001011010010111100101101001000110010101100111011000101110001011100010111001100
0100110101001111110000100010111111000001110011000010001011001001110001011100
```

Taking from 1156th bit for 128 length of key
The resultant key is

```
26 227 144 28 234 94 226 217 225 153 25 138 174 85 90 39
010110001100011100001001001110000101011101111010010001111001101110000111100110011001100001
01000101110101101010100101101011100100
```

So this image of 1933 bytes can act as an unending pool of keys from any length of 64,128,256 or even bigger key sizes.

IV. Future Scope

Keys generated through this algorithm can be an input to any symmetric algorithm.

DES is not considered a good encryption technique because it has a short key length. But with the help of this DES can be enhanced by using different keys for every round of DES as:

B[I] to B[I+L/8] , B[I+L/8] to B[I+L/8+L/8] and so on.

Similarly for triple DES, the same image is used for finding out keys.

Same techniques can be used with any symmetric encryption techniques to give better key lengths without overhead of sending large keys.

The same mechanism applies for every other encryption algorithm from AES to RC4.

Clubbing symmetric and asymmetric techniques is not new. For e.g.: In PGP, we encrypt the text using the symmetric key but encrypt the key with asymmetric public key. But the overhead of encrypting a large key with again a larger key can be a lot avoided using this technique.

V. Conclusion

Till now most of the ideas have been proposed regarding the techniques for better encryption or security of keys. But a major problem faced in symmetric encryption is frequent key exchange which has been avoided for long. The good algorithms are there but least used because of the large key lengths. This algorithm will help in focusing on this very important but avoided to a large extent issue. Unlike PGP, the need to encrypt the keys every time can come to an end. Again it can be implemented for different key lengths and can be mixed with any symmetric encryption algorithm used. The image is encrypted and decrypted only once. And thus only by knowing the position of the 1st byte of the key , the key is generated and used saving a lot of time in encrypting and sending the key at sender’s end and receiving and decrypting the key at the receiver’s end. This saves a lot of time which is a key issue in may time – based systems.

References

[1] William Stallings “Cryptography and Network Security”,3rd Edition, Prentice-Hall Inc., 2005.

[2] 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

[3] Ayushi,” A Symmetric Key Cryptographic Algorithm”, 2010 International Journal of Computer Applications (0975 - 8887)

[4] Volume 1 – No. 15

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

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

[7] Paul A.J, P Mythili and Paulose K Jacob,” Matrix based Key Generation to Enhance Key Avalanche in Advanced Encryption Standard”, IJCA Proceedings on International Conference on VLSI, Communications and Instrumentation (ICVCI) (2):31–34, 2011.

[8] V.S.Shankar Sriram, Abhishek Kumar Maurya, G.Sahoo,” A Novel Multiple Key Block Ciphering Mechanism with

[9] Reduced Computational Overhead”,©2010 International Journal of Computer Applications (0975 - 8887) Volume 1 – No.17

[10] Naim Aljouni,Asim El-Sheikh,and Abdullah Abdali Rashed ,”A new approach in key Generation and Expansion in Rijandel Algorithm”,The International Arab Journal of Information Technology,Vol3,No 1,January2006

[11] Saroj Kumar Panigrahy, Bibhudendra Acharya, Debasish Jena "Image Encryption Using Self-Invertible Key Matrix of Hill Cipher Algorithm", International Conference on Advances in Computing, Chikhli, India, 21-22 February 2008M.

[12] Sharad Patil, Manoj Devare & Ajay Kumar,” Modified One Time Pad Data Security Scheme: Random Key Generation

[13] Approach”, International Journal of Computer Science and Security (IJCSS), Volume (3) : Issue (2)

AUTHORS PROFILE

Mr Deepk Garg has got around 8 years of experience in the technical industry. He is working with Stryker as a senior software developer where he required to send in the patient information to a virtual doctor digitally and securedly in which time is an important factor.Thus he had to save the time spend on the transfer of large keys and their encryption and thus explored this algorithm with the help of Ms.Prerna Garg.

Ms. Prerna Garg has an experience in both inustry and teaching for 6 years. She has explored the subject of network security and cryptography to a large extent. In her thesis also , she is wrking 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.