Int. J. Contemp. Math. Sciences, Vol. 8, 2013, no. 5, 201 - 219
HIKARI Ltd, www.m-hikari.com

Conjecture of Two Finite Fields and its Applications

Tadeusz Ostrowski

Technical Institute, State University in Gorzow
Mysliborska street 34, 66 400 Gorzow, Poland
Tadostr@Interia.pl

Emile Musyck

Computer Science Department
Universite Libre du Bruxelles
rue J.G. Eggericx 18/16, B-1150 Bruxelles, Belgium
emilemusyck@gmail.com

Abstract

The paper focuses on two exponentiations, operated consecutively in two different finite primitive fields with characteristic two. The result of the first field creates in the second field a large number, practically infinite, of encryption algorithms and the only one possibility is the brute force cryptanalysis. In the appendix is attached double simulation of the Secure Encryption Device algorithm for encryption and decryption of 127 bits.

Mathematics Subject Classifications: 11T71, 14G50, 94A60

Keywords: SED (Secure Encryption Device), Cryptography, Discrete Logarithm, Finite Field

Conjecture of two finite fields

A conjecture is an assertion for which we do not know its proof yet, but it is suspected to be true, in the absence of cons-example. Suppose two different finite n bits (n states for Mersenne number), made and operated like a linear feedback shift register (LFSR, see [1] for details). The characteristic polynomials are primitive (see [4]) and thus the length of the sequence of consecutive powers of discrete logarithms is equal to 2^n -1. The characteristic polynomial may be represented by the sum of the powers P^n, for example

$$P^0 + P^1 + P^2 + P^3 = P^7 \text{ for } n = 7.$$

The nonzero-power components of the characteristic polynomial express the numbers of bits from which the feedback loops. By convention, a discrete logarithm has the value 0 for the vector with all bits equal to 1. Each n-bits vector is an element of the finite field. This vector has one and only one discrete logarithm and every discrete logarithm corresponds with one and only one vector. The exponentiation of an input vector to the power K gives, as a result, the vector having discrete logarithm as the product of the logarithm of the input vector multiplied by K modulo 2^n -1.

Any exponentiation of a vector belonging to the first finite field, raised to the power secret K gives first result, which vector, placed in the second finite field and raised to the same power, gives the encryption result. Knowing the input and output vector of the created encryption algorithm, the statement says that the secret exponent K can only be recalculated by an opponent making exhaustive search of 2^n -1 possible exponents. It seems to be possible, because the structures of the two finite fields are similar, discrete logarithms and encrypted data will be linked by a function to recalculate the key K. In fact, when the same vector from first finite field is in the second finite field, discrete logarithms are modified according to a bijection of size 2^n -1 and it gives the correspondence between the two discrete logarithms in finite fields.

Let Ve be an input vector whose discrete logarithm is equal to lgd(Ve). During the operations of encryption, discrete logarithms are modified according to the following relationships

Ve → lgd(Ve),
lgd(Ve) → K * lgd(Ve),
K * lgd(Ve) → bijection (K * lgd(Ve)),
bijection (K * lgd(Ve)) → K * bijection (K * lgd(Ve)).

The last term has the discrete logarithm vector encrypted in the second finite fields. The value of the bijection (bijection (K * lgdVe))) is a function of K. There are 2^n -1 possible values of K and therefore as many stated values for the bijection. We find here an exhaustive search of level 2^n -1, i. e. brute force.

The first step towards the realization of a finite field of *n* bits requires the creation of a primitive characteristic polynomial. Initially, the components of the characteristic polynomial are chosen at random and then checked whether this characteristic polynomial is primitive. Knowing the loops against reaction in the LFSR, we can construct a square matrix formed by the *n* columns representing the first *n* vectors P^0 to P^{n-1}, the left column being the vector P^0 formed of *n* digital 1. We obtain Vandermonde matrix Mv. The latter matrix must be inverted. The linearity between the matrix Mv and all vectors V_i of the finite field is expressed by matrix multiplication

$$Mv *Vd = V_i,$$

where *i* denotes the discrete logarithm of the vector in question.

The vector Vd is called the distribution vector columns of Mv to redial the vector V_i. Knowing the vector V_i, the vector Vd_i can be calculated by the equation

$(Mv)^{-1}) * V_i = Vd_i$, where $(Mv)^{-1}$ is the inverse matrix of Mv.

The characteristic polynomial is primitive if the generated sequence is maximal. The verification of the primitive of a characteristic polynomial can be calculated easily by performing the companion matrix Mc to the power *n*, which is given as a result the initial companion matrix because all calculations are made modulo 2^n -1. This elevation occur advantageously in a polynomial of *n* processes increases the power 2:

$$((\dots((Mc^2)^2)\dots)^2)^2.$$

Two tricks are used in achieving a cipher of two finite fields. The first trick is to determine the vector whose discrete logarithm is equal to the sum of the discrete logarithms of two vectors (the vectors are known, but not their discrete logarithms). The matrix Mv has the left column a column of *n* numbers 1. If, instead of the left column, we introduce the vector which has the discrete logarithm *j* and all subsequent columns, discrete logarithms are also multiplied by *j*, we obtain the Vandermonde matrix MvJ shifted by a factor *j*. The vector $V(i + j)$, the discrete logarithm is equal to the sum of the discrete logarithm of the vectors i and j is given by the relation

$$V(i + j) = MvJ * (((Mv)^{-1}) * V_i).$$

The second trick is used for the multiplication of the discrete logarithm of the input vector by the exponent K. Denote

$$\mathbf{P} = p_{n-1}*2^{n-1} + p_{n-2}*2^{n-2} + \dots + p_1*2 + p_0$$
$$\mathbf{K} = k_{n-1}*2^{n-1} + k_{n-2}*2^{n-2} + \dots + k_1*2 + k_0$$

Multiplying the polynomial P by the polynomial multiplier K can be written

$$\mathbf{P*K} = ((\dots((\mathbf{P}*k_{n-1})*2 + \mathbf{P}*k_{n-2})*2 + \mathbf{P}*k_{n-3})*2 + \dots + \mathbf{P}*k_1)*2 + \mathbf{P}*k_0.$$

In this last relationship, we have only two discrete logarithms additions or multiplication by 2, which is the same.

By performing two consecutive exponentiations in two different finite fields, we realized the cipher complete. Using the LFSR has a very bad reputation in cryptography.

In fact, if you stay in one finite field, all relationships are linear and the algorithm has no safety. By cons, performing two exponentiations in two different finite fields, all multiplication functions that combine elements of both are in finite fields nonlinear functions and therefore we return to the nonlinear sets. The Secure Encryption Device (SED for short) algorithm is a special case in the finite fields of conjecture, with the special feature that the two characteristic polynomials are actually trinomials, which facilitates the calculations. To break the SED must perform tests in 2^{127}, which is likely infeasible. The Advanced Encryption Standard (AES) 128-bit blocks includes, but is not entitled to require brute force in 2^{128} for breaking tests. Some authors suggest the number of tests needed for 2^{115} breaking.

The appendix has been performed the encryption and decryption of the number

1234567890ABCDEFFEDCBA0987654321

with the key

1234567890ABCDEF1234567890ABCDEF.

The left column is the value of the exponent of the bit of the key. The discrete logarithm of each element of the second column is doubled compared to the element which precedes it. The discrete logarithm of elementss of the third column is the sum of the discrete logarithm which precedes the more discrete logarithm of the plaintext input.

We carried out 500 tests for finding polynomial primitive characteristics of 127-bit at random and we found 29 primitive polynomials. The polynomial must have non-zero the term p^0 and the non-zero number of loops against reaction must be an odd number so that the vector having the discrete logarithm 0 receives a zero digit in the transition from zero of the discrete logarithm to discrete logarithm 1. Therefore the number of primitive characteristic polynomials can be estimated as greater than 2^{115}.

Universal test for the randomness of a series of numbers

The robustness of an encryption algorithm is a concept difficult to quantify. However, it is permissible to say that a cryptographic algorithm will be more robust than the randomness of the encrypted blocks will be closer to perfect randomness. Any time, cryptanalysis has always been based on the presence of repetition of the same words, letters or bits do not conform to the statistics. This test is based on the theory of probability distribution of the Poisson distribution. We create one collection of 2^n ciphers after a random seed, each encryption is performed by taking the result of the previous encryption as the clear number and encryption key below. Each encrypted block of 127 bits is used to create 127 slidably n bit numbers, the first number of bit 1 to the bit of rank n, the second number of bit 2 to bit $(n + 1)$, and so the result, the last number of bit 127 to bit *n*-1. By grouping is created 127 collections 2^n n bit numbers, each number being derived from the previous encryption. Is carried out the development of small memories 2^n listed from 0 to 2^n -1. Each creation of a number of *n* bits, we perform an addition +1 in one small memory corresponding to the number listed. After completing 2^n -1 additions to one collection, we will rank all the small stores according to their content, which content may vary from 0 to about a dozen units. The Poisson distribution is used to calculate the exact values of many small memories containing totals of 0, 1, 2, .. 10 units, which are

$(2^n -1) / \lambda * e$ for 0,
$(2^n -1) / \lambda * e * 1!$ for 1,
$(2^n -1) / \lambda * e * 2!$ for 2, and so on.

In these formulations, the coefficient λ of the Poisson distribution is equal to 1 because the number of small stores is equal to the number of ciphers that form a collection of numbers. For practical reasons, we gave 19 to the number *n* which is a compromise between the number of small memory size and numbers of *n* bits.

In a real test, the results do not correspond to the exact values given by the Poisson distribution. The difference between the exact values and the experimental values are compared to the standard deviation which is equal to the square root of the exact values. It then performs the weighted average for the decade of the squared deviations from the exact values and obtain a single value expressed in units sigma σ characterizes the randomness of a collection of 2^n numbers of *n* bits. Finally the operation is performed 127 times for 127 numbers that appear in blocks of 127 bits for the SED algorithm and calculates the average of 127 results. The average result is independent of the seed used for the creation of 2^n -1 encryptions. For the encryption algorithm SED, the test result is 0.57σ universal sigma. By increasing the number of terms of the characteristic polynomial, it enhances the value of σ. The lowest obtained value was $\sigma = 0.173$ with a simulation of the algorithm SED with elements of 19 bits, the characteristic polynomials are not trinomials.

Pseudo-public cryptography key

Strong authentication in the field of computer security, must ensure the following: access control, which can be accessed; confidentiality, which can be found; integrity, which can modify; traceability, which is the author.

Password or biometric verification, are not always sufficient to ensure valid control access to an application. We remedy that state of things by using a digital certificate. Certificates are created by a certification company that verifies the applicant's identity and provides authenticator (or Token). This authenticator operates in conjunction with a public key infrastructure. With RSA techniques, it is possible to create an asymmetric encryption algorithm where everyone may decrypt with a public key, but only the holder of the secret key can encrypt combined. It is possible to create an almost infinite RSA encryption algorithms that allow companies to sell one certification RSA certificate valid for a limited time and require the applicant to have to buy one new certificate after the elapsed time.

There was never any question of creating authenticators using symmetric ciphers because for to apply the principle of revocation of keys, it is essential to have an almost infinite number of symmetric algorithms that is not possible with AES. With the conjecture of two finite fields can create an almost infinite number of symmetric ciphers, the prospects of strong security could make a fresh start with the pseudo-public cryptography key.

Key cryptography pseudo-public does not use asymmetric ciphers, by cons, through the use of a trusted third part Trust Authority (TA) infrastructure that ensures the safety of the above four elements that form the authenticator. Each affiliate receives during his affiliation one secret key, one public address and one finite field addressed to him by the Diffie-Hellman protocol, [5]. Alice can ask the TA a particular key and the finite field of Bob. Alice may correspond to Bob in encrypted mode using both finite fields, her and Bob. The message text is the subject of the creation of a footprint block by the hash method of using the two finite fields. In that hashing method, each block of the message is encrypted, the key to encrypt is the block being itself. The result of the first exponentiation is added XOR (exclusive or) to the result of the encryption of the previous block. The first block having no previous block, is adding XOR block made by the 111 ... 111 or any other block defined by convention. The result of the last encryption block is the footprint. The software verifies that Bob received the footprint is accurate. Sending the footprint to the TA, Bob receives a certificate attesting that Alice's message is correct. Bob can send a copy of the certificate to which Charles can ask the TA a new certificate that the certificate footprint received by Bob is correct.

A new design software sending a message with foodprint safe, one could imagine that the actual message is preceded and followed by a short message consisting of two blocks. The first block includes clear coordinates: longitude, latitude and time of creation of the message and the second block gives the encryption of the first block. For fully secure message, the last two ciphers must be made using a secret key shared with the TA and in a physically protected enclosure. With this method, we stipulle where took place the creation of the message and when it. When sending the request to the TA certificate, it verifies the accuracy of encryption time and space coordinates. This procedure is not applied cryptography public key. In fact, the authenticator can only indicate that the key was not revoked. An experimental cryptosystem with TA has been working with the SED algorithm since 1999 at the Free University of Brussels. Internet users can ask the TA an affiliation cryptosystem, keys to correspond with other affiliates and certificates to authenticate messages (see: http://www.ulb.ac.be/di/scsi/classicsys/experim.htm).

Final remarks

The Data Encryption Standard (DES), developed at IBM, uses small data block of the length of 64 bits and key size of 56 bits. These restrictions are unsuitable for large amounts of data. Triple-DES (DES applied three times to each data block) solves the problem of the key length but it implies that Triple-DES, designed as a method of increasing the key size of DES without a new algorithm, is three times slower than the speed of DES (see [3], [6] for more details).

The DES algorithm was controversial mainly because of its relatively too short key length. Nowadays it is considered to be insecure for many applications and has been superseded by the AES with three block ciphers, AES-128, AES-192 and AES-256, where each of these ciphers has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively. The DES was replaced by its update “younger brother” Triple-DES, which was believed to be practically secure, although theoretical attacks could be found in the literature [2].

The conjecture of two finite fields opens new perspectives for cryptography, especially in security. Key cryptography pseudo-public allows us to give all members a finite field for their exclusive use, which helps to achieve stronger security. Note that all applications are free available to users. In appendix, there is performed the encryption and decryption of the number 1234567890ABCDEFFEDCBA0987654321 with key 1234567890ABCDEF1234567890ABCDEF. The left column is the value of the exponent of the bit of the key. The discrete logarithm of each element of the second column is doubled compared to the element which precedes it. The discrete logarithm of elementss of the third column is the sum of the discrete logarithm which precedes the more discrete logarithm of the plaintext input. And in the line 126 lgd (7FFF ... FFF) = 0, line 125, lgd (7FFF ... FFF) = 2 * lgd (7FFF ... FFF), line124, lgd (123 ... 321) = lgd (7FFF … FFF) + lgd (123 ... 321), line123, lgd (3AE ... 53F) = 2 * lgd (123 ... 321) and so on.

References

[1] E. Barkam, E. Biham and N. Keller. Instant Ciphertext-Only Cryptoanalysis of GSM Encrypted Communication, Journal of Cryptology 21 (3) (2008), 392–429

[2] J. Choi et al. Related-Key and Meet-in-the-Middle Attacks on Triple-DES and DES-EXE, Lecture Notes in Computer Science, Vol. 3481 (2005) 315–324

[3] N. Ferguson, B. Schneier and T. Kohno. Cryptography Engineering, Wiley Publish. Inc, Indianapolis, Indiana, 2010

[4] A. Mitra. On the Construction of m-Sequences via Primitive Polynomials with a Fast Identification Method. International Journal of Electrical and Computer Engineering, No 3, Vol3, (2008), 158–163

[5] B.Schneier. Applied Cryptography: Protocols, Algorithms, and Source Code in C, John Viley and Sons, Inc., 1996

[6] D. R. Stinson. Cryptography: Theory and Practice, Third Edition, Chapman and Hall / CRC, 2005

Appendix. Simulation Program of the SED algorithm application of 127 bits.

Clear message: 1234567890ABCDEFFEDCBA0987654321
Encoding key = 1234567890ABCDEF1234567890ABCDEF
Decoding key = 6237D1861B5975C5F7E86C2444D9F450

```
126  7FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
125  7FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
124  7FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF  *  1234567890ABCDEFFEDCBA0987654321
123  3AE4215F594783BDB9C2565C1E24F53F
122  63993853EB359BFDABB99C434C10A3E8
121  481F47761FBFA9E305A1D2A488603328  *  500DADE73D4B66FB578E552A2B9464F7
120  5ACCF1D496E80B7D20166252777A0C6D
119  28A51E1DC2C4EA9EB546C5703D627019
118  26BE586A0B07FB1B20D9EC5136AABB3A
117  14B66C0464BF495402A23F70CCA13B51  *  4C9DC106116AE1EF4A0731F2365E8012
116  522EBB141306038B39F64A5A370405FE  *  22C691C0262598C8B7C2A1221ADAF71C
115  5B1A1C4689C41CCCD48B1BA7B4BDEE7D
114  546D376707DF5CB6BD87EF5CF8D2122D  *  547EFDF3CF2AC5D14F54C34933E95AC0
113  26604005FFDB3DDFDE0ED66A23A426C5
112  147B8B339CCFCF54000C2B52E0E72B00
111  45908F907DAE1E237BE11D30E1FE556C
110  605BB6FE81F0850FBC2B9A0737382BEE  *  3722577BC9DFB6BF90D34226BB389B78
109  2DBD18E8994EBC5CED481B306DBAAC03
108  26D79FDACBBEC57147869EF550DF68EE  *  2F8578AC3AFC1A753F47C176B9282238
```

107 19CC4FA98C4E99EFDFA5C31FFB974E9A
106 34881D2F523366878DD06EF5477439CC * 020ED1C2B5F13AE6969283CEAA64513E
105 0C173DF629C4ECD99197013AEC950779 * 0B365876B8D28BACB4F9622A147BBB58
104 016E12B79B43BE4553812615725CA6ED
103 70C689F4C5D9AD7F8B9D93EC5FF89FA6
102 4EFDD0498E7B3D6E1357DBB499164F33 * 5DB1F2723A8DC4FE599914930671874D
101 5BE89D370D1842EB2C667D27236E0C04 * 2D51BE8D5AF3E3EBFC167F707326318A
100 55DA9A345C094229A766F11FC8E30653 * 4F5F8B259670114695588C8189A0640E
99 61F16B3F426DE858858881C0FAC6A086 * 7659F7639B7BCDC4CFE3E3C5834DC970
98 4D48A447F282781CB76EB363ED2B2F52
97 51D59D7168AF5F80CDD5B02BBC7008E2
96 2A34D9AB7B19B2C9468255CDA83F70C2
95 166BDDAE1BB899AE8362C874922AE179 * 2DD7B6D7353A97276641EAC402274AAC
94 2AE8D9B0A18A1A71225623A54A7E24BE
93 59960A71E8446D31A4C78D5807A77DC9
92 57774677FD9842C4358F5C6086E6DD04 * 332EC298C88D0746EFB7A3A04C144ECE
91 122116352C297BBD2D8E4DE9FC8D5C85
90 061BD43909442D56EAE319897C9CA316
89 7C77CBA0E950EC79C2BA5F9FD62AA586
88 732F82B32E90643DFAB6A501062C7C44
87 0D2E15C3701A91EEE60945CC8BA32FD4 * 676CE012D2199F35DF2B2EBF12207B99
86 788D76ED3703C6D516EB0748B4CD125B
85 73827D268E7A3A15D2720C23E34AE569 * 77B91249A270D656A157C18AA13454D2
84 7E7093B9052792779818420E254B55B9
83 3C0B71FE751FA045CF952B708527B140 * 459AEF9411A96255A22C3474DBB83D34
82 2F6847AACAC38A6339C45AB678DB5667
81 66F179BF937F6AAAD19AE3E081688B1D * 29618815DE1B9C0773C571A85203BFAC
80 55758BFB7D73CA98EBFBF7A3771C004E * 59C05C0E033248F496E64107B4D581F0
79 24B413306723FEF70C1211179181015E * 13AF2BBF34D49EB731B6F99B6F4A63B8
78 062CA5F225A0930E2D9D199144359271 * 1A05D3268688C42ED604C34B915DD027
77 3498C097E621244AB046B242E36F2509
76 2D5DBBBE233D86BFCB7714C5DB5F5156
75 6526572B5C93A0341B1E1327B04A5CF0 * 5BC3056367BF188D5B7A82701EC77837
74 686F102DC3AA87ED484C500DF84DB1D9 * 1FA06B076AE602D2E10E7B41D16F0457
73 473064C0465DC3717699C47B3FE6E525
72 6F7EEE30785EE0CC50BB5818EC1D4DFA * 6449B94AFB484B9F5AFCEFAD0E500288
71 3463AEB753B66E95CCAEAD709D6C8BCD * 2F987C1212030E3E5FDF47A112A89455
70 290C74704F23C5E736EB3F21F2F7E0C8 * 7C617DF30EC15C19DD93625D928F116C
69 0CEF4B0A701BCE2E3106E3F658EF0884 * 5E3B8B5111430B75AAEF84117DC53DC6
68 2837D36F41615A36F5396CD2CE5D8D58
67 56B02DBFE92285CE6FC944369B9BDEB5 * 30D88D145ECAA3B1D82BC74F6EDF0282
66 5E3D1B82BDD6F99CA8C51EA9682C6EF4 * 11AF133E42CA98C8A83368D6FF134FCA
65 7ACB663DF91E1C045326ED998BBEE271 * 3BC3AAF1181485029F4B5C1CC2202C91
64 5FA0D3E06A5AFDFA34733AAEBF66C0EA * 0B272E8B22D87D1596F8CD58E832BDA4
63 4EAE147ED6F9B16D27E5174C40E6F997
62 1EFA9A08CA5C73FADA46FF8862FA8A29

```
61  04F9FC5547683E8D2E58A810412C339A
60  3CA2F0873CDCA5955C8146B0DC36412A  *  37F70FDB57ADC33FC5AC723A2A2AFC7F
59  5D73FE7DCEFCE7AD9A8059DB20E22FCC
58  54D641EF300440DB2E35C3EDC7439AD8
57  659DE97BA008F6C2E2C33F5C53C2E8AD  *  054D134BA38491CE83184C044D806B8C
56  0C66A216F5ED915368E343A18A382139
55  421378856B14F975026B0A28BA0AA5DE
54  5CDB39E1808EB395B65E3A623379815A
53  68DD149EDF44073840328DC651D089A7  *  3C49AD4A733B4457BBF8EB64EF41D0F4
52  6F20918855196E974D2ED05D6FAFA57F  *  084957B9FBF8CE73532BD577B1272174
51  4D40928965B09FB70393FF711EC87E11
50  5DDA6C0EBA1971BA7B94ADCE47FCA27E  *  11DF4057C6833CF1FED4517791DC53B8
49  09C7D4C15CF3A643DC8680DE1FED0EF8
48  4187DF4CEA5D23F597EEC2D058846C23
47  5FF44F701BFD6DD209675B2AD4E30168
46  64F33DAC6EC281C0F46C3FD64A2BD614  *  2F7D676E3BC01D2BB91278B025D5FE72
45  59F28CEA444DBA37DC6F103FC7DAE993
44  2447F2154D2DF95863AFAED4605BD28F  *  64D9045A9E788CF57709DC15BBD12818
43  04A2D88533609B9977088C417ED1FE95
42  3051A4D9E4BE73A61EDD8BC2B89374B6  *  589F8FA67AF2B8F74A3EC71A1FE5CCC2
41  6881770FBE00648B4CAA0DD69F4E0DBE  *  1DAC70BFEE9FEFF60E2DE4C856AE8EC0
40  7BE756EC7ECE9003CA3947F0C533FEB8
39  30AF0741954606EF7F06E13549C330DF
38  62CDA9FEFC4193CB895A904BF37A0532  *  608F7BD6FA3757BF3879F10BE2F34E22
37  080DB102B3A329490C54DEB2A980933D  *  1994577B88CC16D61A571CA90736DED6
36  448B45AF66B240608272DDE3F675D987  *  18BA8D06E7855A67493C0AB77FAAF539
35  4B7D505AB2E6F379F743435A9867B882  *  001BE8C55686B5CEE06822C945A90BBD
34  4F3CFB633ABEE059AA4A707A92A4DEC9
33  22FEE0D13C9E74111059630534FCA888
32  14E90FC6FB3EE53613D14BCB8EAFC6F5
31  7AA10579CD031F8A3C6D200538951184  *  396119201644871B3F0FCC10EC10C43F
30  134548C9374918CFF577639E80BE0B61
29  76126F9A5E4ED285214D91453B411E00
28  4187061749F077986434610926E6B055  *  654ECA2B92ABF88BADD3D6F481FDAB3E
27  77995E39ED6426608AE99563C0727153
26  42404775A8F71F88C92ABBAFE4487701
25  5C1B93F3AC4E72589572C272F70F4D7D
24  6823086F491FF2D3A5EC5E0BBEE7677E
23  0570E711CD708A3E62490730F1DAD92C  *  579D8B538E0AE2E35C4B164492F678DB
22  1573B7E47EAEAA207104CE6AC4E53BE1
21  0699B2D3A24FC8ACB0CA65FA66ABD8CF  *  327C1CD6EB76A1EFCEC23D107442BC31
20  122BB0D0C41119863652BE795804F5FC
19  79142990523E19FEDC9C353A3748404B  *  6E5B01CF6E4364544B4429FD9BF9056E
18  75CB67A130F42D3D8AF8AFED7490A56F
17  31ABE16EB8736B06E1FDC2A0192ADFEB  *  40DF642D9A4374ACB2D9B1989D9E875D
16  6CC12432885316D78B675021715D69D2  *  505626D9FA1E35AE078E941D239CFDEC
```

```
 15  19F3A578D47A2888F3A804F422A466FB  *  2DC10F9D4B21D979D7AEA368FCC7E0FC
 14  5A1720F93E3384E56D5124C4D789BCB7  *  01E7BA5022B9B9AAD27037F81D0C326E
 13  7F0708BC5F64550CE8E6A0779FB45AA5
 12  30C1C072FEB2A02F58C14B6C99AAF2ED
 11  523DDF081CCF4E160FFAA2D657C3D9FD  *  2D5126AB1F303E5312C6D43FADB22915
 10  1915993AE4B5A56EC8012130E00B6AD2  *  0BC357BF1FDC70EB9FCBF4FBD95F19F7
  9  419FE321A64F9CFE37C324D082F2F96F
  8  2304470F37DE14FB574B6EFC74123007  *  518B9C1DBCD0FD60AB9ACA640675B74A
  7  6538B15388DF07D753121AFEC01574FD  *  3EECE529784FCA577FDAEBDDBDA9CBFD
  6  1FC63AD2F465D94A8F8C5EF0ED986A7E  *  643DDF7A7F775E22C2D94C55F0FD7E06
  5  3793D31BE4F240A770F2724E68F42B16  *  0D36C5592BD9C0CA172281829AE0E941
  4  0E16E1B6D0655746D96C178BDCC11197
  3  013B06BAC8076E8AE633B49566426389  *  5AC5EE0D9D34B7ABD1B9A842BF6DCCE8
  2  57692094FA07FD24BB1AED51A24F5553  *  0408971EF41E8FE39C888F8403B13A4E
  1  3CA0C2BD867E3BC63D9F083A4ECC08D3  *  1396123DF76BB082AFBA1E37CD78C695
  0  35DF757BCAE4D0D4C27289936DC14C15  *  4E2529D14D714E4EBB2F08FBEE38E77A
```

RESULT OF THE DLM ALGORITHM APPLICATION =

```
4E2529D14D714E4EBB2F08FBEE38E77A
126  7FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
125  7FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
124  7FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF  *  4E2529D14D714E4EBB2F08FBEE38E77A
123  2856ED18813E8648056469B8FA20D84A
122  67CADBA9A5244FBF1FD40B9973A1CF54
121  0267F4C80149DC5CBF16339C10FF5556  *  781FB67919A9566A2D9B2312BE0E1F4A
120  14EDDBD113969AEB51E5871C63FEA8B3
119  4C85FC55A62704685BF607E2D2D8C888
118  2DD666C219C19C74EB6CF5DEE94746DE
117  7B36A28E86ABEBE51ABCCFA0C9BB13E5  *  0C570C6EE60E4A0C3439C0D65EB6B296
116  0EA877C38FFE8ABBD3E2CEBCA90CC53D  *  6A39C9F1F9B379233FD69314D3D14024
115  0E06133ADD691AB09369EB1AC879EDB0
114  4370BB5D8328823496C021C59AEDCF60  *  09A6C14A619E5093256E697A9F34CCDE
113  75B53CE3C2C4BFAAA278E94F10E8EB9C
112  3593DFA11B24B0F884E6FAC705364589
111  27A89C2299D4EE21602D68BDCE2A415C
110  45879374DAC12E720905ECAC57FB2D8F  *  5B47109B7055B01833392FE7F3B8C8B4
109  69110E5A957E6238668FA84769474F51
108  45C4DF1FACA1C858A4A3482756F94CFC  *  521EE6DD72E3D9C12C5218D3155D19A0
107  14F64D0C643F6AEE84CB33ED623C3580
106  5E288ECF70F1FAECDA0A6E7016B2419E  *  3E3EE5B0A48F7C65AB32D8833AE511E6
105  2D2EF7756DBF3E71085563D49A8403DD  *  6C60A966ACEF36E00DE9E3D086D30409
104  1F721ADC03F1F506DE4374F11E3006A2
103  75E437EF38AEE762FC7A711987A4D472
102  060839D3A69C9C43A1A1CBCF74B658F3  *  5F59B0B8BDFE6AF7D0A239A118449B6E
101  737ECC6BF63BAC7C8241B05743D6A485  *  22ECBA1BAF68BBAD6533EB8B70B4AC53
100  43CCF70985285930C11950C8CD762D6E  *  2294F618FBC49D4A47476FB32C5067B5
 99  57B8B7BEBD60309692964B07A3C636B4  *  345E3923E67384BAD396F21DA391EB2C
```

```
98  6A8E22C31E94046BD46FDAFA052972F7
97  0CAFC5006A2B7E4A07D294C4C6F498DF
96  79C7EAF33D30F657165AFEC8BC276BE1
95  02DDAC34819C895EAF880BA14329839B  *  7AAE0188C3BEA3F1AB8A684932C69C2B
94  3357B95444C056BC89149044BD8812AE
93  393CFCD7449E2E50B60C47380514D285
92  2F42668E57C68840662C9D488D6AA64A  *  2EEF8475D76D8527E65E149A8A1E064E
91  05DDD59A7ACF23D2C6ABFC047E44317D
90  09C2CACE0671FFD7C66228486F02BF8D
89  09DDA46BED47CEB9C3788794C81E388A
88  1790C640A62622B0F1580462163EC0AB
87  0162ADC186565A139D4270049798CB2E  *  68EE8ECB3BA51EA2EE8F1B9936309FA0
86  6503416105D1C444915DF160BA783466
85  2364ADEC1F1CBD8737B3C1DF8ED1C5A4  *  07413B14321EB5A4A52A169109148971
84  4BAAED521B24C49D7942E2D138BD2104
83  20253013040D13037046B66B73831FD0  *  1FBF89FB0BBC3BFF9798A8DA5582C25A
82  24A1A3D8CD20EBAA354BA0130E0C2DD3
81  715551282C66628E9F7DFE97F2F5F2F0  *  64A9B62BBD26DBB07817B81F22E29C8F
80  203F9CDFB6419C7EEA0D03F53B8F5F60  *  3CE635FF40BE0B881C7F84779ADA2D18
79  1B8838784657A73FA3AA8C540C949DBF  *  67089D953D215FA4CC42CEA766A31763
78  6977D014F0E2CC58BA2532111CB8BC68  *  6A2751D2DCDB8CB0C5F3DA5ABCC30D68
77  102A1EF7EC33AC32C8697010F90B5D46
76  773E5AC4C681FAF8E05B1956D2733044
75  1B98542F1C44B35CEC93C0E88E99D656  *  31FFB0492B926511338FC46D52F28AD4
74  76882761E857BCF3348AF8953F2D1549  *  0975570C1AD9C1276AD24F6A32CBE309
73  24D50D12576744CDF0949157826F613B
72  6718A4D0DB7AAB383E6A3CF8A3E28FB0  *  239C0FC629E0C6B387A4177C5D7D0CA4
71  585FB3CE04A12188526AA0750096B437  *  1018CB3DD917A0A3D7F336A8F54526E3
70  0D587F77174352B8FEB5504B6DA29B97  *  32D07921561F7B59D92C39D54EB64A1D
69  723B6CF1E9DBEACAC9635123B6B3E20C  *  23BB4AAC6837B721C7F77A3F06B37583
68  704606D9403591809E23577159522797
67  3DE21596AB46DF1CB242CD6BEBC64539  *  371B38C62ABEF563633BC60C508D4D11
66  2591704FE9DB87765500C10D5092FCFA  *  7401EA0534785DD53DEF301202AEC826
65  0FF5FCE171001C8A07954AE510DE1425  *  703C0C9CB36CC4E26040B7F5DD229867
64  42784E18A959E6AA15F50BEB3DA1DC27  *  5B9A72ADCD05F9B9043ACCA7F8957C6F
63  7829EE2D7690D5C1E1C724B5406FA49F
62  7DFDEFC16A56B75537E042FFD456DBE7
61  0EA7FBE657950667ED37CCDCEA2E6459
60  02ED695E16F0EA111AAD9485C231CC23  *  69362E844FA06095EEAF36258EF7A21C
59  0304B29F0EBA6A53BF0306A64A73E3E8
58  286761911E5B2C242F53B91062681AD8
57  0B7EAAF0363A9CE1BD8C5D461C537227  *  2A21BDF0EA9971ECE4026AC3D790ED98
56  0251E78BDD4D6FEF9527BAFEFCEC3A27
55  3D348A5FCE4AE61A8669636997AA73DF
54  3FBC3B5D45E9435A5CD9ACB3A769EA07
53  2BE8F5DA4B775688345F5CA3852A1E46  *  1D28236FB34B0E89DB05F03A62DC13F0
```

52 722E87CC0099EE54226CF20FFB11FE9E * 13A29F6B33D0296590BC334D388DEDD7
51 24E0C98E0F76B0ED17BEB8EA04F5ECA0
50 633FD7832E38E2AA664EFF33E36ED218 * 3DD6779C677F6817DA756A793A5DDB7A
49 73B438B35CAC27DCE9D24D9273A9262A
48 053C0AEBB68A3B6A5EF1ACDB6A2212AB
47 33FC9E842AF76A36A55213F2056CCAD6
46 33D2ACF5829000F387CCC510EF4D74C3 * 57028267FECEFF58281A2ADB5FE1887F
45 0AB81DCA732AF3CEB3F9841A395E5999
44 4F6F9825D85064320E5AD21BAA5BDDDB * 58826FEC8CF29E937C1B039EC4D36B1A
43 460E7DAF1988459B102F6C9124CE8435
42 7C81EB78C2F6BA9D13AE909B21D78ED2 * 1E57970F6951FAADB50112BA8AE206EF
41 2954E6031B1357B346ACFC72183CE519 * 18EB361709333149033DCFB1BF8F3A43
40 0010F7F26EE64EFA49F8468091CDD670
39 4F5C0647D03D4006A284776D8AA43F78
38 2DECBFCFC6C75B75BECCD3C809F95FA1 * 11CC9490A3E5EF3292347CF774293F13
37 24938F51DF9687275950732297871A8E * 57B42332639FB456170DA5A606BCE5E5
36 63471915CA2A33DB9FBB519163CC1A32 * 312FCDC1C900D53106BF17AB5C025C1A
35 66432E011AB9ACC8ABEF878C55887A35 * 739B8221A266E3FE45FD961176562878
34 2E2A7E6DA522051AD923B4BBECC63FC1
33 75C50BEE56D1302E648F69C27678719D
32 4230DEE724C27075DEC5DFB83F1BBA74
31 6A1A902D921E4FB8081EFC4E4832394E * 49D8B266DEF81758820C94D530E7CE00
30 460DF96F24D6F4AAE9669A5F968467F9
29 635AA3A4BA52339FA4C5402FBC3FF844
28 522971B2CFF98D1857EF881807C7CFD6 * 13F032100799678B45B081F4A01BEC18
27 31AA3080DE0418D15260642E1C9665DE
26 2A8BC5985BCF8CE5E5E8BADDA2340BFA
25 1DB39CBF364C8C0C4BEB90D67F37F9CB
24 56D0052FC37F74BA41FF6EA666440F48
23 56639F80C49D4A3C43BA2828669F50A7 * 5962BCCD3863D4064B5168CCA769FFFB
22 30B1336324C10F112A2744C201F86636
21 154A0C3EA836F013981D9E47BBA40F25 * 1A422DF0B565A3645C6DC71696797BAE
20 3211A36B8E416324BB5DD9BCBE29AAE5
19 37D0AB938BA3AE6ED003EADDD3357DAB * 5D5972C3AB40747C4B26DAC406F91178
18 48AF13BD6BB2882F863A803B6504C63E
17 203A71CB587877AF25CC985691A211E5 * 55BE2FD1270A861ED4B7FB23102E13C1
16 1328A946602F6A6F7B600C9BFAEF9065 * 3054AE75DE87BD6E31C73CB9B78DBA68
15 777D89C76FF6D1BBCF3FDEF257ABBD27 * 740B6663DE48F88F1E0B9D5E0CD42925
14 63821F564275538398E8F2CE72BC8DAA * 7E739BD34B28CC43B14049B67A5D65AB
13 511CB7982F3BAF42262A32753A5234D0
12 0DA5EACD970C3F54F04DB49590D0957E
11 0081D0EDD736A2AC42816B78A34D41E4 * 0AA6DDB529F5D3B8724756AC50874A7A
10 476C4FDF52BAAD0FD300D9B8C955B853 * 2F9FB35D3DB80EE9DF601E6A4F6B4C54
9 0D8722061A1BBCCA2F66DD2EC8F654B7
8 0B1EBC5CEA0D0D6310A080C5AAAEB0B9 * 3D17FAA9299CAE822117854F13C5E3DA
7 6C036321B9CB48817CF617D463F7F24B * 42DEA8464ABB38704528FED71E73E420

```
 6  364AF3277E1AF4A0E585BF11FBA9F460  *  772090259D16347753A3C17358663BDF
 5  2CF1D21797FAA6F6B3BE25DB88286B86  *  084C4AC32C36E247CFBAD9C0CFAC2C34
 4  6919D62B142217809719CA960C9788A9
 3  43270223972CDCA4070F3B27A720CD23  *  44B19C07EA5D38DBEBC7C5B55F7C8D12
 2  7D566E2789B5D6B54D8721F121151C8C  *  0BD63C5200B8BB4891A512CC61E496C6
 1  456433CD1CECF1085BE5FBD13D2377A4  *  194188110F0347FEF443FA528698FB57
 0  18D65189FE33B50D59DD3C20E028D4C1  *  495686B16E434C371B0CBF1BED179672
```

RESULT OF THE DLM ALGORITHM APPLICATION = 495686B16E434C371B0CBF1BED179672
RESULT OF THE SED SYSTEM ENCRYPTION = 495686B16E434C371B0CBF1BED179672

```
126  7FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF  *  495686B16E434C371B0CBF1BED179672
125  02570108D1F885CE1D7364BE233BA10A  *  5D3A33F0E96A31CD4F3985FA26AFAC94
124  509EEFDBA04D9FABF23B4D1E4A88A537
123  677271D12F0CFC1A49334740B44A9147
122  573C8896C847567EA93630CB2482B020
121  4ADD7143F6E16EA9742EBF8CCF19F467  *  50AD0A085E3257F3EB454FEF99AECE87
120  1AA8A9B52899FAF9BDA42D6368E4A639
119  2E0BB2281314C388DAA70456D45C165C
118  0DB2CBC09FAFAB248D29D5F19AC5D46E
117  39736ADA7353F97DA254EFD40AD7A2FC  *  5692643507AA72D8D619BA89C497B239
116  0B5D824237B338C3EFC92347C88BE9A3  *  3B1D2DD7C29DDC8DCE658362CE87F36D
115  691BC24A21EEBB8AE91D27A1E090A30D
114  7D431C0AEA2653E583E0DA9F2DF10093  *  4237E5379109A080C03EA534361DB8C7
113  6E01961CD5D4912E6F3A62742FC177C0  *  5A727AE6D131057B0268F6F95BB48896
112  78723CC6F924803B55D04ED140A0A2C2  *  45631DF84FC9B464DAE683D6A82F012D
111  12537BC2DF97F4DD4AA7F360E7850A8C  *  40FF1DDA07BBC92CDFCB7F6CB66D7741
110  1207F6D738073C8F37222514A746D185  *  564AE372462151679111A2B46E7989D6
109  5B7CFD1C2C0CB729C505B9DA47440AC2
108  6854FE2A365DF4544E40B7B066AB6992  *  7CC0A57D1501E8639FD399AE5DE9A1FD
107  5A078CF7DA3C331BCBF5E2C3D47C7E6B
106  772F80D3840B0988132FA1F7D985C4C9
105  1D716C87AC1A1947F3C221CDF030F73C
104  6691EE15939A716A67019087073E9789  *  50C1F456A5C3EC19BADD2BD6D8D2AE58
103  56550A6A94B66D4295DF12F2D2FA4DBE  *  1447E46D72ADCDEBA53AB85CCBF55DAA
102  344B71CAA8262C6F76AF98B3340DB2B5
101  3EDD5507DBA7288890C806F44972D0B2
100  456097399FBD1950513CC7128B0136ED
 99  32FAF01097BEFB72C6D10665113B1D0B
 98  11A50D1A9FA3DDCCFA9B0FB084730757  *  03E639329060A2C4723A35FB819CE3EA
 97  38F270327135FFD62005C3E97B901B4A  *  79288C56906BC2892EF25FD7C0D27165
 96  1302FF13D39F8B218E06EAF25964C233
 95  391D81A2FAB518EC35BB3DCE91EC1716
 94  70B42E2EF0120F7CBD7A1CEE03271D3B
 93  378CA7D26588E483FE7095DF65F4EFC8
 92  079C47674555F5873A4C1EB6FB606F5F  *  165281951E5F3308D6FAEBB96F32F7A4
 91  1545784CFD36505ABC80E89298BFB257  *  37198AF476FBDC6975CCA346393697BD
 90  412B88EF5208B1BB8842EEC2BB464E0D
```

```
89  40A657ECE4FB0992CE56D65A4E9B876A  *  78A96EDB30835023BEDC171AD6351A03
88  2E031391FD46845574BD892A823261E8  *  212ACE621D91BC8A47A562B269B977F3
87  5047CBACDC0D5695DCDC29A2B8C1988E
86  6D9775F794A45594B1BE907C5C413F63  *  3B7B7D4C7AA19392F39E53E45A40BD44
85  7F68241A530FFBD1ADD24981366B57D7
84  35158B6A312447E496C5C4B12AD9ECBE  *  0623938A5D1BAD198B63DF8B035C5D07
83  2130C4766C19C0B08190B58E4A7299BF  *  7C9116A5E2E2115F3984453859557016
82  71BC202FC84CE9A1CA5B52D4BEE784DA
81  08CBAA50D36CF2B7501D7BDFC1D1722C
80  54E7FBECDFD00B86699BED7D58959377  *  56870952D6FF5149ABFA8016C97C5C9D
79  2AD7E634B8181ADA8F3B586FB3915D92
78  2778EE28AC58237E5169BD655415A372  *  503A676EF32E8C9E72F037DA672CF6BF
77  47137EE608C60C4BA25974F7615B3787  *  3761DA572253FB2D490AD8C4A6494ECB
76  575B6154925E8FC92BC3D0A55703694F  *  258D09C4D089519E112C41C8747B51CF
75  1B05750E480470C040B05FB75485F17F
74  28074F1855F9CEDF4D30B8539902B87F  *  3587D07A66F1D3AC3EBBCAE0A04107A7
73  681B505608D2FC194DFE287CE1DE3238
72  50F3E1FC6AA0200E827A14046895F7B8  *  2E9659BEB2EC4A56F2137F02E9EB3C74
71  7F1462893FFEE18D7ABC1CB111EE58CE  *  6E4E6F299CE87F946C9F12D677F55970
70  5B7724669B0A94DBA721E72B5244D89F  *  01DA5A45B888EE9C1FA8848A754A2AF9
69  1A1E33414048C0CBDECCD0B5F4CA9E43
68  73E36F09751EB755E730E92ADA03A9E8
67  1C5F777F1AA48CB4EA359E6FACA21D27
66  64B3F7323C642519AB1133F5FC7495C7  *  78F5F3F51741BA1B42627A4142AB6A7B
65  300A3DF2404C5664D194AD2F3B522657
64  6AFA3D2ECB14EA9F76514CF413C5AAC6  *  403C68EE859757F11F815B25D3889439
63  7D9FA19D2A571455EAF7B93F24B011C4  *  1ECD6802202C48D630FF8EE712861737
62  16991E1FBF7CFA5F036CA042653E96B8  *  2366B2F608A253C4C538A025231E3F1B
61  0FAB08275279944D140963FC11F9644E  *  56AACA7A0992F4AB926F5C560522D926
60  5D13BA80D209AD227E2CEC72EC248BDC  *  6AD6581AFE8EB8581C9DD83531646A3F
59  6389246DEBBE68D4971AA429A2B40986
58  3D389C332A3792DA2BF3295018DDA7BB  *  21FD28E19BD9D5272677C39717F38C96
57  125BBED80869C2D97D399E97A088C4DD  *  4AC9837DE49D3D85C4A0CB40798DF29F
56  71AEB27E8EC92E1E405BA70C18F32598  *  067C2E8C52559A6A31D049BDBFBCA71D
55  0905EC9830BC578A4801B7F14C2683EB  *  11257E41ED32016724C20DC9BC82AF7C
54  15C8F06B817217423617400B4AE13F88  *  756F63F907E91E5944C21D65866F7590
53  50517613FBF33DD441BDDC98A0D3DC80  *  2D5754B8F88560C320BC148BAEC823D4
52  0C7ECE6E1AB13F57AD7D08A1F20E74D6
51  356D5E74E0DED27A7F6A0765C6B70ABA  *  3F5CCDE926CA22E467056FC3A8937C97
50  5BB899B35B0671EFD2BF5C8F39F6BB46
49  7572B7F92D90DEFF77DC013B484EAE3C
48  26C67208180511C950D9C902B49A09F6
47  34FF13DB8F3B019549313BCB9F44675B
46  2F25091AE9AF90B7C200CE37A4593228  *  56F63375E53F96E8A0D2ED899F5ACACA
45  2DFE92ED1CF4395BDA07525310B570CB  *  1B783AE08278D9A8DF240838410203BB
44  73870DB07F5FE821C9FA99ED9E77D056
```

```
 43  0EA59832DDDBFB0C42625EC1F2E1D4DD  *  1B92AF3D1B47D029E4DC760F080FB69B
 42  1DD0F21027258706FEDE66E1D724A3B0  *  34575FBC6F5AA377C16FF352262543FE
 41  779CBD79868F350A13C5F43550101FFC
 40  1A89E83380C810CB34E002981C1E0671
 39  76C97A00198CA5BF82719A1B81A5A09D
 38  2193DE85BDB5E3B7A19DAA2DB461438D
 37  2DFA25F5CCCC6B0DAED045FB2E11BF75  *  536FA572625AC6F6059F44548AC39BF1
 36  00342586B65054CEC0CAE80823AFE084
 35  76190EB2833999398BEFD281E26159AF
 34  3EC99CFF92F2D9FB9DF3A46554222D07  *  07ACAA659D1D6FAA58DA6F5D97619F98
 33  55D97434449ECA6DDAA6DD83A3E023BE
 32  0A332C22958BBF91D40865801471D005
 31  74D018D8444A387E62A85F1D95678654
 30  438D53202C66FC15A4B34259C1BA2AA8  *  4623145BC1E7B50A829A42AC20C3D3C1
 29  21ECC235CE6D55700B9E88160D6F907C
 28  60CE3D84D8A603227892DA99A501A00E
 27  4038C2EC95CB25BC2BB51E7DD3FE7962
 26  14C9AECA827C3E75F371F99A21C34475  *  5F48F79D96013FD7B8D19025C254FF02
 25  57A1737BDCE18BD5F18BCAA907E09FF2
 24  06FBC72E772ACD5D07B9FD9EBDE1F90C
 23  7859B62200125C62C9F47C639E3A80F7  *  1C30ED1A2520CA65C831F155F51317E3
 22  095990E400FCB2AB9F3305171AC783E9  *  551EC968D4708AF5B5937341832179A1
 21  51345A96A711560246090D9B59C3D3E3
 20  4FDC7F3D0175C4373223F60F8D69FC76  *  11DF6B52F29EC632484A04EE266E6ECA
 19  28A04EB40628FB1B8A3BBC83C4E4F6B2  *  11B47215883727AA030A6D7601C22F3B
 18  198E9F35A28B3EC4079C081414871631
 17  6647C59061387D301CD739B91CDA0E9B
 16  039172C0F1A5CE23640F6BCC7EE2A450  *  4D753CAAB48640C4662A9606C0D7EC78
 15  5A2214CCBB45F9BB76610B5F82EFD9C6  *  468654B2BE2F899252168D2F775EF04B
 14  4AEDE4C2C16C949940A6CB856701B749  *  47B3748FF68FBAB53BDA2B046C11F489
 13  70280DAD8D30E1B0256FE565E74EA743  *  68552F700D68C472343A36E9D7994597
 12  70CFF62A16BB1CA38AC1A5C4D7CBBAC1  *  0C5D792DE701880747AA399408097BC4
 11  2E3E2D538E5A5AD618DE00DB26501628
 10  1C417583F9988C3694222D0665459346  *  73AD4E84B298959219422CBC9EBC139A
  9  65A2C9F20A8F2E713C7CA9F78489DDD2
  8  0FF6586F2D22615847D75EBC6DF392F2
  7  28201338D20530083B147EF7A3156113
  6  17C89CD04064E0A7AD97033525E48317  *  056E018E6591C147C3A0416EBC74095E
  5  706855862E1D5C854F96212818C2B583
  4  57665AA26C1A8D4183C097F330ADA1F7  *  283C9B8D85C76FBB2CBF0B1A781AF6A9
  3  7497306767497A3421D8045500BB34A2
  2  75E26BA1802FD32CE798A9D176A92B8C
  1  1C3FDDD9555C6D7B46BB534494CE38F1
  0  4E2529D14D714E4EBB2F08FBEE38E77A
```

RESULT OF THE DLM ALGORITHM APPLICATION =
4E2529D14D714E4EBB2F08FBEE38E77A

126 7FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF * 4E2529D14D714E4EBB2F08FBEE38E77A
125 1EC42B9A29BB293552D57D399D07A1FA * 67FACEA1D5E6EA01C019870BE60B6F84
124 7B4C0066DD0A98CBEA5BFB750558C0F8
123 70A152E33C0FB7851B190196884E216C
122 723E9B3AA925FB11DCEF32C0927F7FAA
121 412BEF35775DEC9AA97ADB67CF6D3ACB * 38B318B39DBD4B3C8627BA87961B37E4
120 1C4E5DD2F88251D084E79016A16D23EE
119 38105DCB97E41625F3B240D4A90819C1
118 23B0353C54DB1E9CB5B337AC35BB1B54
117 641CA2C012A510E0A661E75E0B097821 * 51AFD22B5D30435E190212D22A542527
116 563796F3D51BD96E68E92D3C6F2198CB * 5FE0E833F96DD9215F1A8DFACBA834AB
115 2BC3C73ECAB0EDD03CB6B6EB28452B05
114 66A3E023D3B11036E2A9610E3A141AFC * 4574A49D3CFE3FA1CACDFD47B4D6BCCB
113 1F5A716E686D7BDA201DFC372FFC58F7 * 7F6E10EB2F4BBC3DAFF60B56ACD4816F
112 3FFEB60BC93EC55119F16D935F2C1024 * 4541757730F12873DB744F77D8C48F56
111 1CA9A03542597E4E1E0E3106E980721C * 3F2EB3A54DEA62E15CD865EF5167F222
110 1CFD16F59E20989A61143667BB2608F5 * 267CD39DF84F04FB06F50328D93D82E2
109 6784B02DE62074E80C7F913EC0620F52
108 04B3B39E6233EADB08881BF3BD9DC570 * 5FE5C38FF2DCBE729DDE624A87A881A6
107 5B00F86B13EF8E3FFDD5D8DD63F782E9
106 1B620FCDCCBC8592C5E3F5F3B23410CF
105 075D4BE73EFFDDE4DEDE6CDE7C5489E9
104 7C7E6BE5AE9CF7B2D3F53F331BD4F75E * 1CE79DEF3B4E10674062F145B7D0A019
103 382EF48F7BE4F5F2E0A1AEF435034B8E * 35DB7128BE9AA6630DE80103E92FA918
102 5168D892B239258163C977A654B87BD1
101 15058681D48D8A26912720851897BF39
100 3655CCAB4CB54C0826A24EE74267D789
99 22B46558E1ED65615DD16E55A2233D7C
98 57E9919078A968B107F806EA4B6974C5 * 4AE42A17F38CF849DEBB123931007E7F
97 6D6AF75FE554397F02E04E2EC37051BB * 385CB7A32C7E381E30E65FE898E4F9F8
96 1C70A421A2406722D5207FF4D3BC04F8
95 38DF42019BA0EB3B9824A3F047B118E9
94 1F8E27CE50D8F0C874605B3236511C5C
93 0BCF4E38D4B01E34560DE882CE3EDD7C
92 41932E0D9EC4D0BD25A1910F08CBE19C * 6803EE0AB0B1C5E085686FE9F1337737
91 76B3F3DC3534015AA131ADC8E3A70BFD * 61B0D805561BC2C0DEA309ABB1453D48
90 38C751C1174F3CA95A87FBA3EF291C0E
89 2F7210BE9638E0CAC94DAD02E3DE5575 * 7510E068101D50B0C7D4427298D5DAA8
88 0D59F6C2FB0C898C35FF07E5A5C16DCD * 35AD9FF53B6FDC1E2FB691E97CF1BCB5
87 1D576A24B70C01592C9149C0EB133408
86 4429A58D4958DBA26E41C1EC3FF59746 * 751A1D8232182EE98AF13587F415B53F
85 31A6FB5B0428BCE421E4FBB0D9F93647
84 12346889CFA154AEFFA01A726F12075F * 2DB7C8ED4636121F67B47C9D1561CF9B
83 15E45E73DD7D39EA5F74ED4BC91707C2 * 2AC2FD3AABFA535C9BD5023E2D5FF084
82 1699ECE6CCE5239556A33F549912A82D
81 45B5B7BBFA11087A111E3765DB20B9A5

```
80  1CA89E9891809C600F5409FAC17C8F98  *  0BCAD46E5605FC9DF98433B842CCE03B
79  4D60219A169F75CBA9B730A70CEE47E8
78  2E1974C02834BB68CA4AB43D4158D160  *  491FA8485811FB0B0EB5972229232F6C
77  52BACBCFA5706D436BBFC53B305E3162  *  612FE590C5293718A1C125AC8DAA3ED7
76  4436E53FFB6B4931EC9625491DB1384E  *  0BC71F63C6A9553B2B57E07FB48A1A02
75  7D6C1F82C8CD482F23866A7599AA206D
74  0329492F0BF3B3D52E4DED16514C1A3E  *  71580071E557EE1EEA359C3311D4EC4C
73  7EF95B8C3F0C72F407A99A7CC6F83806
72  703933B59B5F4120EFFD32E3B215C1AC  *  2BA07A03804FCCC887F0AD68D957ACA7
71  19A057FF439BCC1FB3FCADC0E1E2117E  *  2AE63D7ED27D3AF803A52B92C5A0B5FA
70  6A9A0BB81CE5433516247FD5DC65C340  *  411FE5BC98152288DCE3B0269D1DDFF8
69  5036F8C33B6B531DB783F99A24E6727D
68  26F0E2B9334D2021DC9145ADA6D1FBD8
67  64860DF1C42A5F7621D251E6D7FC2734
66  04527FB8011B3D071F5C156458C28D74  *  110FD4AFC58CFF25828925C0BA264A00
65  363901CC15AD65CCEFA74D1EC301E867
64  61B41F4A0CC712EC0A9755DAB454DE22  *  082D37DEE7DF17B3E23F32762A51A036
63  01B3E5E6124C17CA08BFDB02C573AE1F  *  1C4E8A889AE13F6F7E0A7A9102A1C845
62  7BD09D36B1AA7E7DB86934C9D0F28ACE  *  0E6DB5CC1139A1435B7698A2083EE56E
61  3134491891A41DE335092F47A7F590EE  *  16043F8097E7F93A0E5AF6A8CC107ED9
60  45BBCF931F00430D7673C8B33F46209B  *  7F7606F39C0BC13EB6240BE005D8248E
59  73327287F0B50DE348EFFE6FECF92305
58  31DE2DD48116408F32319D5AF214C4D2  *  4A90ED8209421191598BC1D4A73CF103
57  529976C20AE7B02BFE7AAF2709077539  *  346C6B7FAAD3A34E7918C71449FE3A3F
56  6D6F892F45AE4C3396991A2367ED6D37  *  16DD3FED6599C1A54D24A622C1B75B80
55  0AB9281523C039D9B89744881FF4546A  *  0620A71E46A5EAA3C768DB7014E9B800
54  407BE8F2977DF4F793765864C596A71F  *  5FF7F1B28896198BFC76D52BEEA81EEA
53  58CF027F0EF75219828D7584F748719C  *  648286119BB5686A6893A55DD2A2C753
52  076E8C25708B093848539165458C7964
51  0FBE8A3942202B957EF27261FD461F83  *  36A736B141A37E0106A8FD504BF500AF
50  2E4698B1DE76AD0550F4ABED800BFFF9
49  5904A07587BD62C714F88186AAD60356
48  24893052640F4E644F83931AB815137E
47  14AE4176EDF359E4875FC2C2A1F84450
46  3AAD5508A3C97245F5DB3221A7BB3B6D  *  50FDED079827B296B05E83C26BE1814F
45  6AC1C024F6E5334F744FD7809E15468A  *  7875B6AA281827238FBE5CB76B2D57BF
44  33BFB25BA1B65AA8E5B0C48F18B118DF
43  2E2F9FC35DE46BA067F49E7B9469AA81  *  4B8B1E57B98EEA5298A7ABB854F66C53
42  6D9C8D5D37FB9AB36F77B2FA09A79AD6  *  1DBF1BD78308153F5E38C57D9D87D4DC
41  741490FEF49FD6737011CE7F0565D3FD
40  3E50C69D85C1FF09C152B8CFE58BBE12
39  2FC8A50ED04677DB8C5713C4FFC2F274
38  2A0FE282A4560206D90FA34B827C289F
37  266B323C341AB0EAABAF5977C0D7F349  *  63E9036D064C9F808097A62DE408320A
36  38230A490FDDB5153C48A21E44CF8C3E
35  108FDB2D02A761493E3F27D8929A0A66
```

```
34  09F1423FD7A2DAE5CCE9544D74F5AE7A  *  3DFF237C58B5F119385539474BC2C97F
33  23E703FEE8DE4C1C588E5D5801060846
32  571FCB7E031CCFC9CA42273852D3041C
31  16BD34031D5E80FBC3DEC4E2EDF0EDB7
30  75855FE62E5003DD0B1A6B058CC2CCAC  *  76B695A72D2C8DFB29315C9E00F93B80
29  7E499D8A7564A44D1525E921BDD8FC62
28  43F85184B714BD68B2A687929B5351E9
27  602C308C69CB7FAD92BDF9526CDA464E
26  07CF26DCDE3D7E1F867BDDA1B0009A17  *  22FCFDD27FF65AB0C5B6DAAB87D9FBD0
25  57D5CFE13FE7E5D74FF3C2876B9AA1CE
24  597FE557EDC0CB0613CFC4BCC468D6BD
23  187A7F00F899A9B30AD82C3EE292007B  *  6B7A5DDA3EEDA5D78262073B80E0ED4C
22  366EBF67ABEB1B681FF539EB64ABD940  *  55640352207FAE469BF2B90381C7FC8A
21  29A9B8930321562B1BCC70CCA9CBA0BA
20  1A47657493BD7A21CF121839957826A2  *  168020C4CAA4C7BD7F7F76835CD4D3AB
19  494A73CFD702EF9DED9654AE2C4C9326  *  0915A48F60B56DA05B33CD5E96FE72B5
18  0E49C65B54617E0288F26E95B61864CF
17  7208A288E378A4A1699C84CA7F3433D5
16  3ED4FDB19419BD4EFB22B341575E9BF9  *  167C8CDD2400CC29B32FA6B203481014
15  4547731EBD2D2429D7603C3E2EDCD5BB  *  78BF115BA9D8A9C388DAF80D50877C09
14  73829FF2350597636A47D47259B7E02F  *  0096B7A6FD19116590BC6FA7698DAD1A
13  3CF24A4AA183687500250885F60AB794  *  2BBD8F391A2B167DB2D906CCC54D263D
12  555F60EB82FED08538A7DAAE0A7880E4  *  36EDB845CABBAF9C8114851192A6A06C
11  2EB63518934CA094E296509395CCB812
10  26FA6DB4E16607BEB921522D64C14662  *  7993B9858F2F3547A214956C21BFC318
 9  737489D053878CA841F1D5312D5A5F4F
 8  7D12415DB24425C35AEF4CB0412DA67C
 7  0326CAD75CC558E89DD7906CE4AB10EE
 6  701D1B751159264E5822DF96A781398D  *  7E5C90C1961B76945F0A2D5FBC56ABD6
 5  0F3B64E2B5CE10C87A77346EBE4546A3
 4  7101D05D745134256E57EEF4390D1173  *  22E2BD1780BE62FF5EC10B6A95168015
 3  6BE5C7E6A325C54C70CE6CC7B8D6C001
 2  0A9004A82CBC38B668DE1BA72C9691DC
 1  31A9BA0C0C6E9A8329D1AF20DF4DA1B7
 0  1234567890ABCDEFFEDCBA0987654321
```

RESULT OF THE DLM ALGORITHM APPLICATION =
1234567890ABCDEFFEDCBA0987654321
RESTITUTION VECTOR OF ENTRANCE = 1234567890ABCDEFFEDCBA0987654321

Received: November, 2012