International Journal of Current Advanced Research
ISSN: O: 2319-6475, ISSN: P: 2319-6505, Impact Factor: SJIF: 5.995
Available Online at www.journalijcar.org
Volume 6; Issue 9; September 2017; Page No. 6264-6265
DOI: http://dx.doi.org/10.24327/ijcar.2017.6265.0906

Research Article

MINUS ONE CRYPTOSYSTEM

Kureethara, JV* and Mangam, TA

Department of Mathematics and Statistics, Christ University, Bengaluru, India

A R T I C L E I N F O

Article History:

Received 12th June, 2017
Received in revised form 3rd July, 2017 Accepted 24th August, 2017
Published online 28th September, 2017

Key words:

Cryptography, Private Key Cryptography, Cryptosystem, Encryption Algorithm, Decryption Algorithm

A B S T R A C T

Minus One Cryptosystem is explained in this paper. Encryption is done by converting every digraph in the *plaintext* to a single letter. Once the cryptosystem is recognized, frequency analysis is done on the digraphs for decryption. In the usual cryptosystems, if the *plaintext* is of length k, then the number of possible letter combinations of the *ciphertext* is 26^k. However, an advantage with Minus One Cryptosystem is that the number of possible letter combinations of the *ciphertext* is only 26^{k-1}. When we apply the encryption m times, we get the string length reduced to n-m. The number m acts as key and can be chosen and exchanged using any convenient Key Exchange Algorithm.

INTRODUCTION

A world that is competitive demands privacy. As the end of a competition is always the victory of some and the loss of other(s), it is the strategy that determines primarily who the victorious is. Strategies have a component of secrecy. Secrecy and privacy are many a time indistinguishable if not inseparable. One of the earliest methods of the strategizing is to communicate obscurely to all but the intended recipient. This is the birth of cryptography. Cryptography is the study of secret communication methods. It is the study of methods of sending messages in disguised form so that only the intended recipients can remove the disguise and read the message (Koblitz, 1994).

Minus One Cryptosystem

A cryptosystem is the body of the messages to be transferred (*plaintexts*) and to be retrieved (*ciphertexts*), and the rules of encryption and decryption. One of the earliest extensively used cryptosystems is attributed to Julius Caesar of Rome (Koblitz, 1994). We now see a new cryptosystem, viz., Minus One Cryptosystem. Consider the 26-letter English alphabet. The numerical equivalence of the letters is as follows:

Encryption

Let $\mathbf{P}=P_1P_2 \ldots P_n$ be a *plaintext* of length *n*. Let *f* be the encryption that encrypts **P** to the *ciphertext* **C**. The encryption f is defined as follows:

$$f(P_iP_{i+1})=P_i+P_{i+1} \pmod{26}=C_i, \forall\ 1\leq i \leq n-1.$$

Corresponding author:* **Kureethara, JV
Department of Mathematics and Statistics, Christ University, Bengaluru, India

Table 1 English Letters and their corresponding integer values.

Letter	Number	Letter	Number
A	0	N	13
B	1	O	14
C	2	P	15
D	3	Q	16
E	4	R	17
F	5	S	18
G	6	T	19
H	7	U	20
I	8	V	21
J	9	W	22
K	10	X	23
L	11	Y	24
M	12	Z	25

This means that from the *plaintext* P, every adjacent two letters (*digraphs*) from left to right is taken and encrypted. In effect, every letter except the first and the last is used twice. We see an example now.

Example

Let the *plaintext* be **P**= CRYPTOS. The *digraphs* are CR, RY, YP, PT, TO and OS.

The encryption is as follows:

f(CR) ≡ C+R ≡ 02+17 ≡ 19 ≡ T (mod 26)
f(RY) ≡ R+Y ≡ 17+24 ≡ 15 ≡ P (mod 26)
f(YP) ≡ Y+P ≡ 24+15 ≡ 13 ≡ N (mod 26)
f(PT) ≡ P+T ≡ 15+19 ≡ 08 ≡ I (mod 26)
f(TO) ≡ T+O ≡ 19+14 ≡ 07 ≡ H (mod 26)
f(OS) ≡ O+S ≡ 14+18 ≡ 06 ≡ G (mod 26)

Hence, *f*(CRYPTOS)=TPNIHG.

It can be observed that R, Y, P, T and O are used twice each in the encryption. This should be taken in to consideration when we do the decryption. Decryption is perfect only if we trim these doublings.

Decryption

The decryption is as follows:

For C_j, $\forall\ 1 \leq j \leq n-1$, the decryption f' is given as:

$$f'(C_j) = P_jP_{j+1}$$

For each letter of the *ciphertext*, 26 digraphs are possible. For the ciphertext we received in the previous example, we show the working of the decryption. We begin with the first letter T of the *ciphertext* TPNIHG.

Table 2 The possible *plaintexts* of the *ciphertext* T.

19+0	**18+1**	**17+2**	**16+3**	**15+4**	**14+5**
TA	SB	RC	QD	PE	OF
13+6	12+7	11+8	10+9	9+10	8+11
NG	MH	LI	KJ	JK	IL
7+12	6+13	5+14	4+15	3+16	2+17
HM	GN	FO	EP	DQ	**CR**
1+18	0+19	25+20	24+21	23+22	22+23
BS	AT	ZU	YV	XW	WX
21+24	20+25				
VY	UZ				

Similarly, we can go for each of the letters. We get the *digraphs* as CR, RY, YP, PT, TO and OS. From this we can find the *plaintext* as CRYPTOS.

The name of the cryptosystem is proposed as Minus One Cryptosystem because of the reduction in length of the *ciphertext* in comparison with the *plaintext*.

Cryptanalysis

Cryptanalysis (Menezes, 1996) is done on the *ciphertexts*. Once the cryptosystem is recognized, frequency analysis is done on the digraphs. It is a general information that TH, ER, ON and AN are the most common digraphs in English writings (Menezes, 1996). Hence, the corresponding letters as per the Minus One Cryptosystem are A, V, B and N. Although, HT, RE, NO and NA also can be encrypted as A, V, B and N, respectively, they are not frequently used digraphs.

Hence, in analysing a large *ciphertext*, presence of A, V, B and N help us in identifying the *plaintext*. Once we get the *plaintext digraphs* as TH, ER, ON or AN, we can find the *digraphs* preceding and following. Proceeding in this way, we can decrypt the *ciphertext*.

DISCUSSION

Let us analyze the advantages and disadvantages of Minus One Cryptosystem.

Advantages

Some of the advantages of the Minus One Cryptosystem are given below:

- In the traditional cryptosystems, if the *plaintext* is of length k, then the number of possible letter combinations of the *ciphertext* is 26^k. However, an advantage with Minus One Cryptosystem is that the number of possible letter combinations of the *ciphertext* is only 26^{k-1}.
- Minus one Encryption is a direct process without involving difficult computation.
- There is no key used here for the encryption.

Disadvantages

If we continue do the operation *k-1* times, the string becomes a single letter. It is almost like a no return stage. Hence, even if the encryption is repeated for the same *plaintext*, it is not advisable to repeat it more than *k*/2 times. Moreover, Minus One Cryptosystem has all the vulnerabilities of any other Private Key Cryptosystem.

CONCLUSION

The cryptosystem described here is a direct and easily executable one. Although it does not use a key, it can be make key-enabled cryptosystem, if the encryption is repeated. When the encryption is done k times, the length of the *ciphertext* becomes n-k. This key can be exchanged using any strong key exchange system.

References

1. Neal Koblitz, A Course in Number Theory and Cryptography, 2nd Edn, New York: Springer-Verlag (1994).
2. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, A Handbook of Applied Cryptography, Florida: CRC Press (1996).

How to cite this article:

Kureethara, JV and Mangam, TA (2017) 'Minus One Cryptosystem', *International Journal of Current Advanced Research*, 06(09), pp. 6264-6265. DOI: http://dx.doi.org/10.24327/ijcar.2017.6265.0906

****