CETA Workshop Abstract Submission: Symmetric Key Cryptography JJU-256

Josiah Johnson Umezurike

06/10/10

Introduction

- JJU-256 is proposed to enhance the encryption of data with the aim of embarking on a simple, yet a subtle algorithm.
- Problem of frequency analysis attacks are tackled with random and sweeping moves over squares
- The constant short words like, ‘is’, ‘it’, ‘to’ and other short words are mitigated against break in by permutation of the alphabets and/or characters.
- The permutation disguises periods arising during frequency analysis.

The Basics 1

This symmetric key cryptography combines: SUBSTITUTION CIPHER and TRANSPOSITION CIPHER. In this proposition the algorithm will be analogous to a knight on a board of 32 squares. We are not limited to these squares and variables(alphabets 0-25) at all. If you will, we will implore the knight in the process of touching all other squares (0-31) without repetition forming a sequence of infinite permutation.

$$ {}_{n}P_{r} = n!/(n-r)! = 32!/(32-26)! = 32!/6! = 3.6549496 \times 10^{32} $$

n = number of squares. r= number of alphabets on the squares. The equation is true for all real numbers n→∞.

$\lim\limits_{r \to n} {}_{n}P_{r} \neq 0$: Limit does not exist and mangnitude for the permutation increases.

$$ \lim_{r \to n} {}_{n}P_{r} \to \infty $$

The Basics 2

Imploring the knight again in the process of touching all other squares with attached alphabets (A-Z : 0-25). The square counts are from (0-31) with repetition, in this case we also form a sequence (quasi-sequence) of infinite permutation.

$$n^r = 32^{26} = 1.36112947 \times 10^{39}$$

Increasing the number of squares in concert with the increment in the repetition of alphabets and character will result to permutation of infinitely large sequence which equally increases the odds of breaking the encryption. See equation of delimit: $\left(\lim_{r \to n} n^r \to \mathrm{oo}\right)$

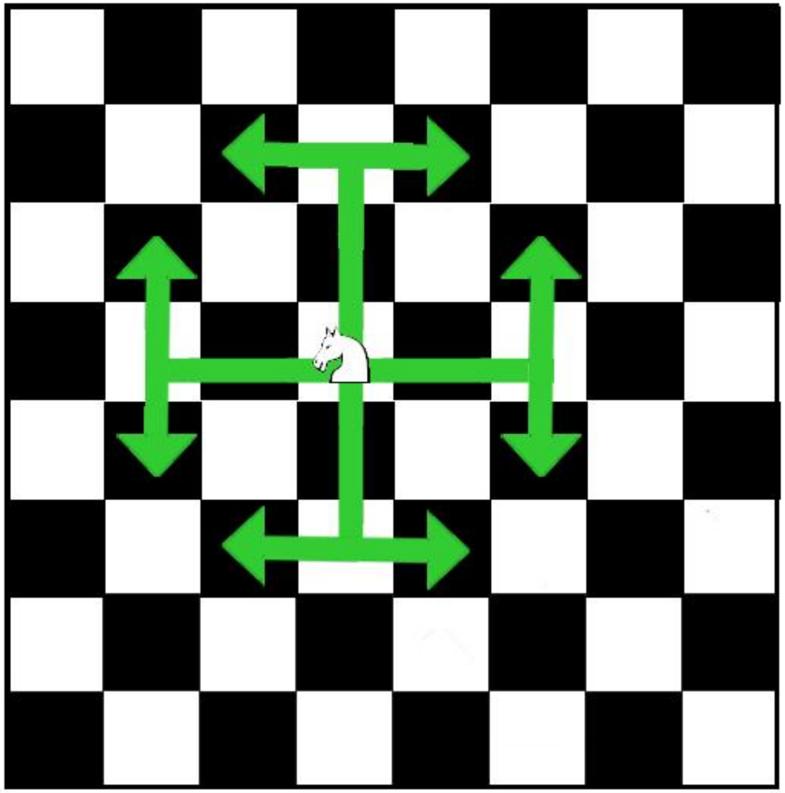
n = number of squares. r= number of alphabets on the squares. The equation is true for all real number n→∞.

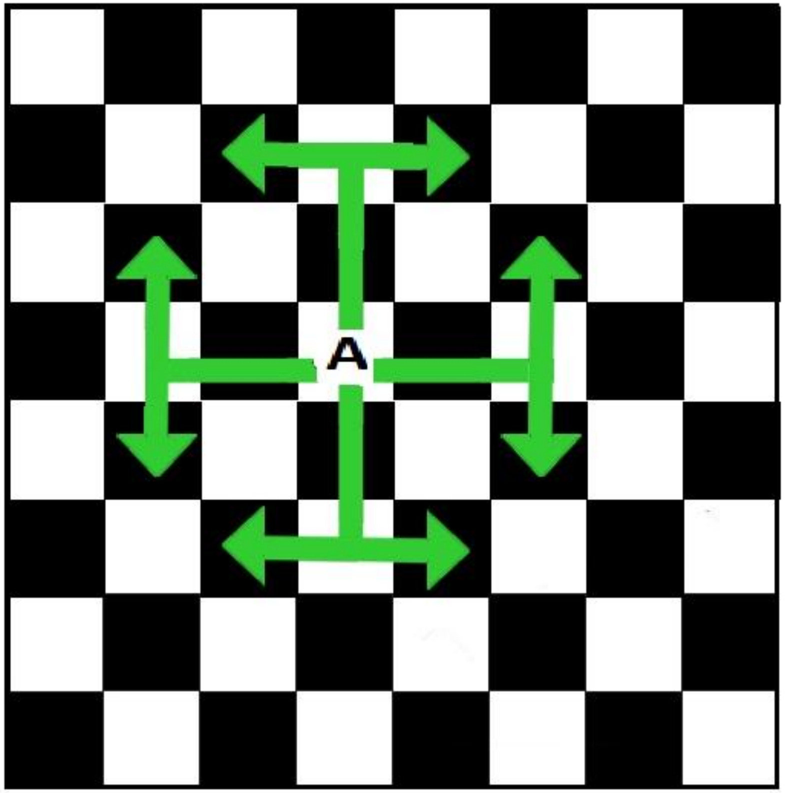
Explanation

- Fundamental characters of the data (bits) to be encrypted will replace the knight in making distinct, yet random moves.
- The squares will serve as the engine in which data (bits) are transposed and substituted.
- The AES: KeyExpansion, SubBytes, ShiftRows, AddRoundKeys and MixColumns rounds (9 rounds) are accomplished in one move.

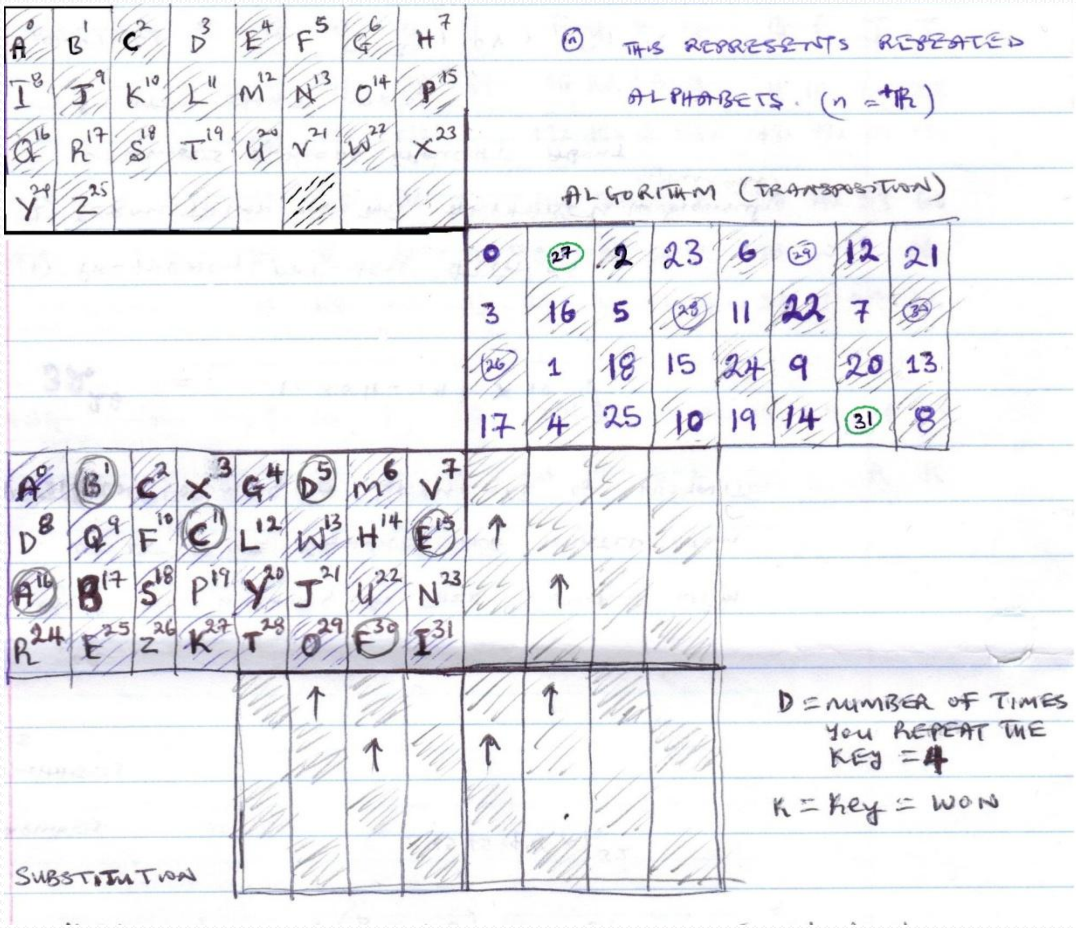
Practical Approach

Knight' movement **Data' movement**





Transposition-Substitution



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

(n) THIS REPRESENTS REPEATED ALPHABETS. (n = +R)

ALGORITHM (TRANSPOSITION)

0	27	2	23	6	29	12	21
3	16	5	28	11	22	7	30
26	1	18	15	24	9	20	13
17	4	25	10	19	14	31	8

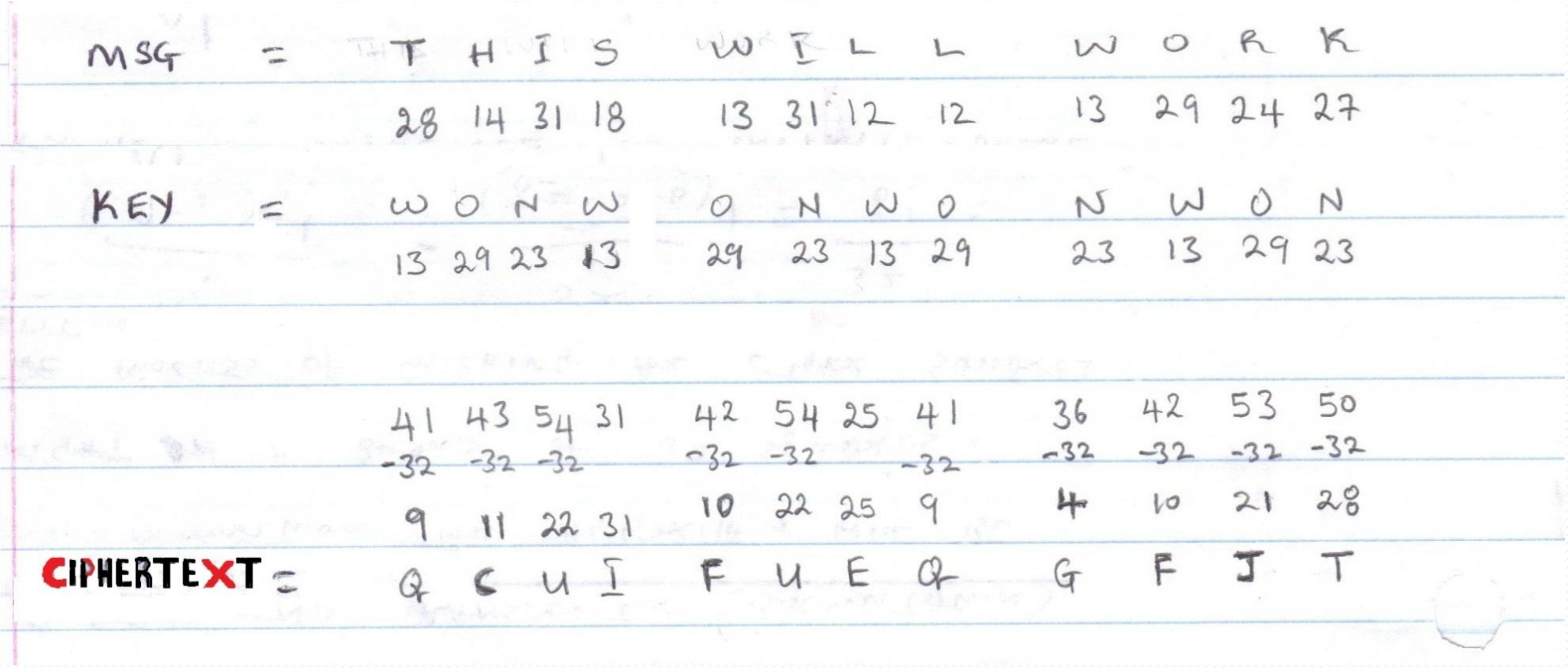
A^{0}	B^{1}	C^{2}	X^{3}	G^{4}	D^{5}	m^{6}	V^{7}
D^{8}	Q^{9}	F^{10}	C^{11}	L^{12}	W^{13}	H^{14}	E^{15}
A^{16}	B^{17}	S^{18}	P^{19}	Y^{20}	J^{21}	U^{22}	N^{23}
R^{24}	E^{25}	Z^{26}	K^{27}	T^{28}	O^{29}	E^{30}	I^{31}

D = NUMBER OF TIMES YOU REPEAT THE KEY = 4

K = Key = WON

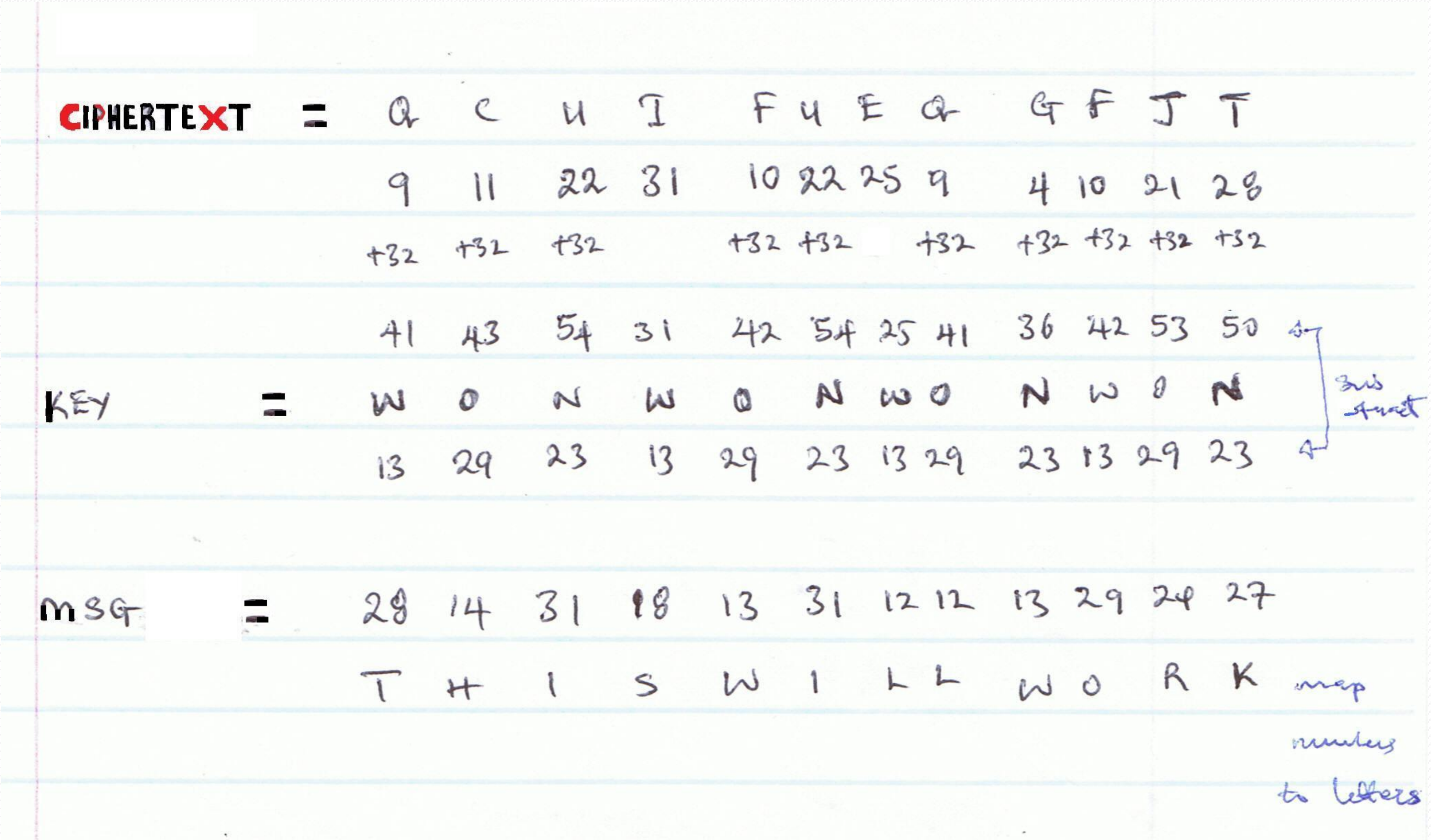
SUBSTITUTION

Encryption



MSG	=	T	H	I	S	W	I	L	L	W	O	R	K
		28	14	31	18	13	31	12	12	13	29	24	27
KEY	=	W	O	N	W	O	N	W	O	N	W	O	N
		13	29	23	13	29	23	13	29	23	13	29	23
		41	43	54	31	42	54	25	41	36	42	53	50
		-32	-32	-32		-32	-32		-32	-32	-32	-32	-32
		9	11	22	31	10	22	25	9	4	10	21	28
CIPHERTEXT	=	Q	C	U	I	F	U	E	Q	G	F	J	T

Decryption



CIPHERTEXT =	Q	C	U	I	F	U	E	Q	G	F	J	T	
	9	11	22	31	10	22	25	9	4	10	21	28	
	+32	+32	+32		+32	+32		+32	+32	+32	+32	+32	
	41	43	54	31	42	54	25	41	36	42	53	50	
KEY =	W	O	N	W	O	N	W	O	N	W	O	N	Sub tract
	13	29	23	13	29	23	13	29	23	13	29	23	
MSG =	28	14	31	18	13	31	12	12	13	29	24	27	
	T	H	I	S	W	I	L	L	W	O	R	K	map numbers to letters

Questions and Conclusion

- How can you assist in this project?
- What are the weakness of the whole inception?
- Do you think that a mathematical approach is better than a visual approach?
- What formulae can we use to identify the movement we perceive on the squares?
- The subtle nature of this proposition could be a strength in time and cost of breaking data encrypted this way. Increasing the key size, cipher block size and using other character (IV or Padding) will increase the bit adding to the time and cost to break in. This will serve as an open source in cryptography with different or differing outcome even with the same encrypted data.