Nature-Inspired Cryptoanalysis Methods for Breaking Vigenère Cipher

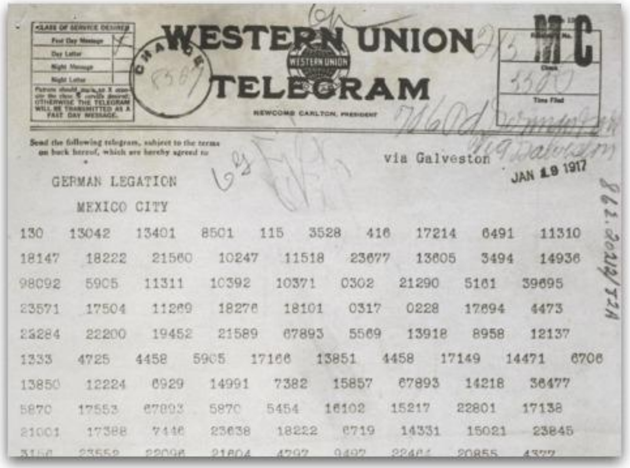
Authors: Lucija Brezočnik, Iztok Fister Jr, and Vili Podgorelec

Faculty of Electrical Engineering and Computer Science, Maribor, Slovenia

Cryptology

cryptography

The Zimmermann Telegram



CLASS OF SERVICE DESIRED
Fast Day Message
Day Letter
Night Message
Night Letter
Patrons should mark an X opposite the class of service desired; OTHERWISE THE TELEGRAM WILL BE TRANSMITTED AS A FAST DAY MESSAGE.

CHARGE

WESTERN UNION TELEGRAM

NEWCOMB CARLTON, PRESIDENT

Receiver's No.
Check
Time Filed

Send the following telegram, subject to the terms on back hereof, which are hereby agreed to

via Galveston

JAN 19 1917

GERMAN LEGATION
MEXICO CITY

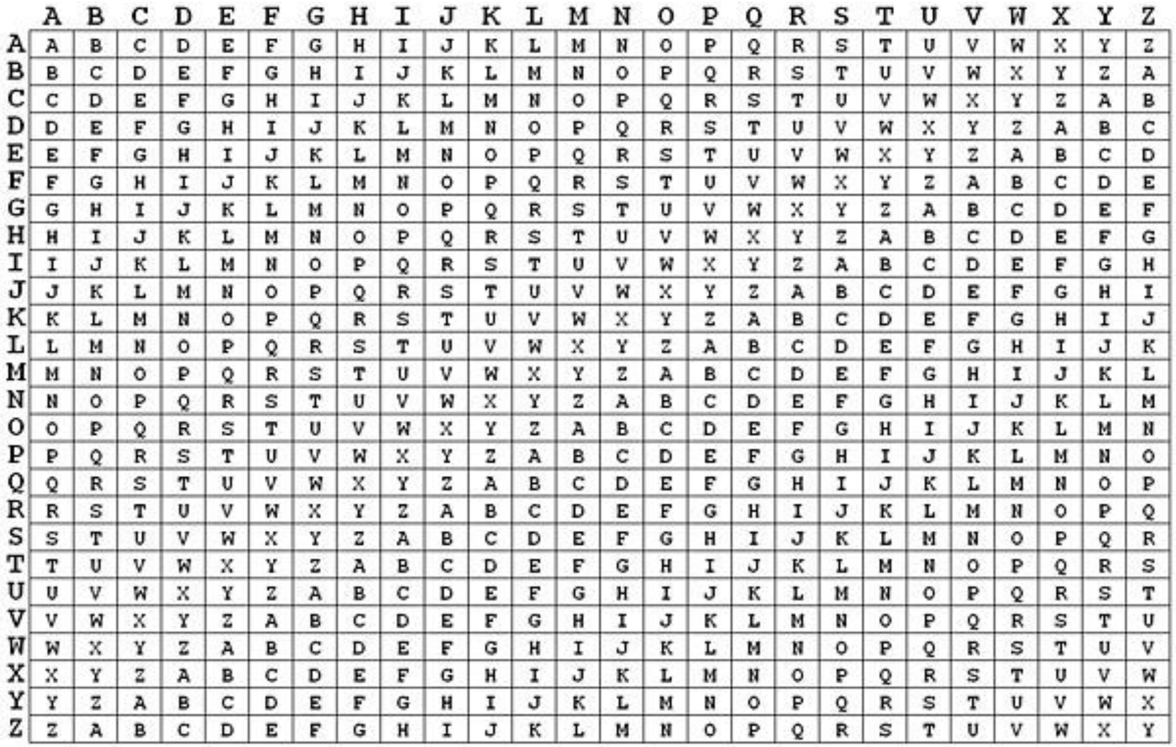
```
130    13042  13401  8501   115    3528   416    17214  6491   11310
18147  18222  21560  10247  11518  23677  13605  3494   14936
98092  5905   11311  10392  10371  0302   21290  5161   39695
23571  17504  11269  18276  18101  0317   0228   17694  4473
22284  22200  19452  21589  67893  5569   13918  8958   12137
1333   4725   4458   5905   17166  13851  4458   17149  14471  6706
13850  12224  6929   14991  7382   15857  67893  14218  36477
5870   17553  67893  5870   5454   16102  15217  22801  17138
21001  17388  7446   23638  18222  6719   14331  15021  23845
3156   23552  22096  21604  4797   9497   22464  20855  4377
```

862.20212/[illegible]

cryptoanalysis

- Classical ciphers
  - transposition
  - substitution
    - monoalphabetic (e.g. Caesar cipher, Affine cipher)
    - polyalphabetic (e.g. Vigenère cipher, Gronsfeld cipher)
    - polygraphic (e.g. Hill cipher)

Vigenère cipher



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Plain text	N	E	W	T	E	C	H	N	O	L	O	G	I	E	S
Key	K	E	Y	K	E	Y	K	E	Y	K	E	Y	K	E	Y
Ciphertext	X	I	U	D	I	A	R	R	M	V	S	E	S	I	Q

Vigenère cipher

- Definition of plaintext (*P*), key (*K*), and ciphertext (*C*):

$$P=(P_1,P_2,\ldots,P_m);\quad K=(K_1,K_2,\ldots,K_n);\quad C=(C_1,C_2,\ldots,C_m)$$

- Encryption *E* using key *K*:

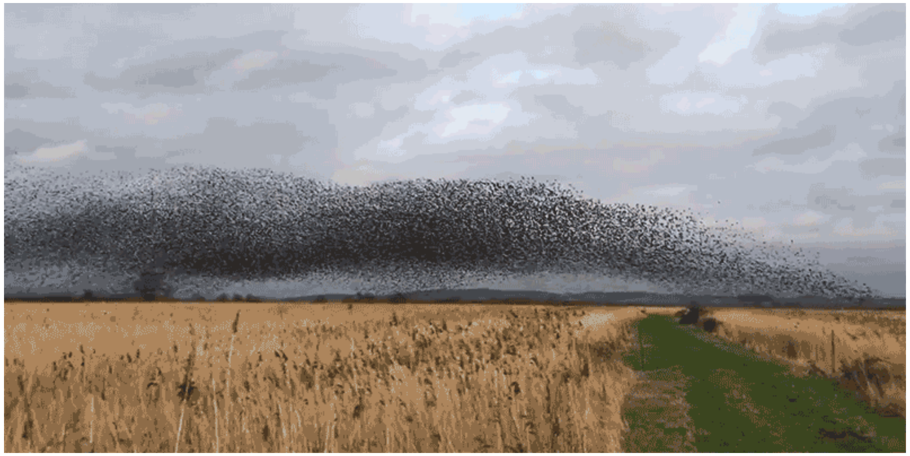
$$C_i=E_K(P_i)=(P_i+K_i)\ \ mod\ \ 26$$

- Decryption *D* using key *K*:

$$D_K(C_i)=(E_i+K_i)\ \ mod\ \ 26$$

Natural-Inspired algorithms

- Differential Evolution: Storn and Price (1997)
- Particle Swarm Optimization: Kennedy and Eberhart (1995)
- Firefly Algorithm: Yang (2008)
- Artificial Bee Colony Algorithm: Karaboga (2005)
- Cuckoo Search: Yang and Deb (2009)



N-I cryptanalysis methods

- Identification of the period of the cipher
  - Friedman attack based on the Index of Coincidence (I_c)

$$I_c = \frac{\sum_{i=1}^{j} f_i(f_i - 1)}{n(n-1)}$$

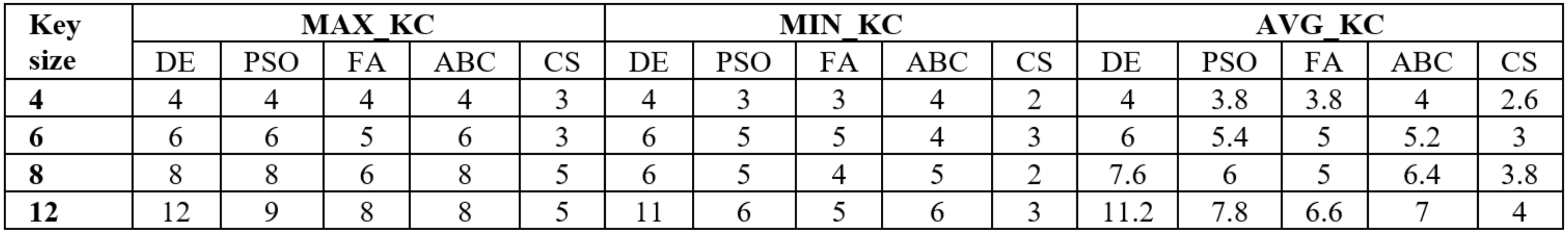
$$key\_length = \frac{0.027n}{I_c(n-1) - 0.038n + 0.065}$$

- Fitness function

$$f(K) = \sum_{i=1}^{j} |FE_i - FD_i|$$

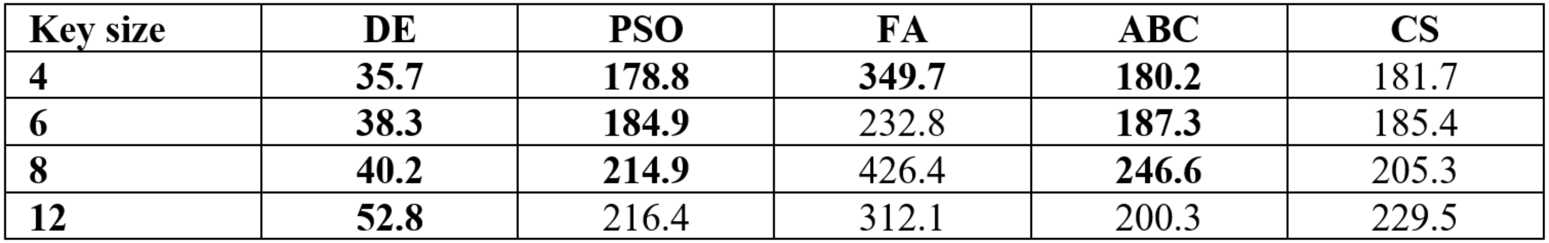
Results

- Number of correctly recovered key characters per algorithm



Key size	**MAX_KC**					**MIN_KC**					**AVG_KC**				
	DE	PSO	FA	ABC	CS	DE	PSO	FA	ABC	CS	DE	PSO	FA	ABC	CS
4	4	4	4	4	3	4	3	3	4	2	4	3.8	3.8	4	2.6
6	6	6	5	6	3	6	5	5	4	3	6	5.4	5	5.2	3
8	8	8	6	8	5	6	5	4	5	2	7.6	6	5	6.4	3.8
12	12	9	8	8	5	11	6	5	6	3	11.2	7.8	6.6	7	4

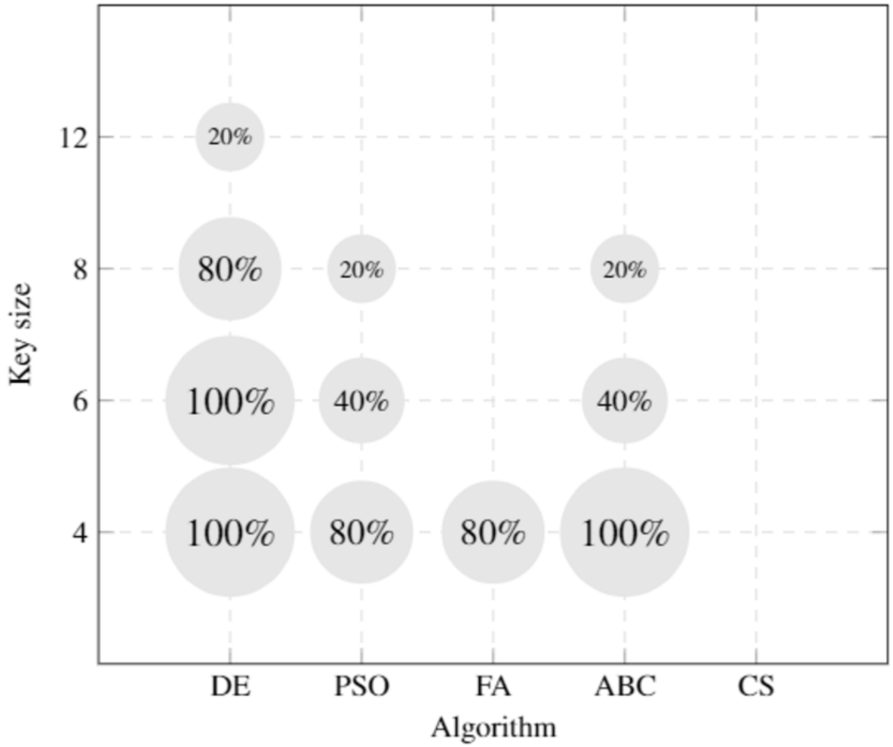
- Time analysis of obtaining the max number of correctly recovered key characters



Key size	**DE**	**PSO**	**FA**	**ABC**	**CS**
4	**35.7**	**178.8**	**349.7**	**180.2**	181.7
6	**38.3**	**184.9**	232.8	**187.3**	185.4
8	**40.2**	**214.9**	426.4	**246.6**	205.3
12	**52.8**	216.4	312.1	200.3	229.5

Results

- percentage of all correctly obtained key characters in five independent run



Conclusion

- Proposed method for breaking the Vigenère cipher
  - Tested with four different key sizes
  - One plaintext
- Best performance: Differential Evolution algorithm
  - Recovered the highest amount of key characters
  - Took the least amount of time
- Future work
  - Utilization of other nature-inspired algorithms
  - Utilization of nature-inspired algorithms to modern cryptography