Caesar

Lecture #2

Caesar

The Caesar Cipher technique is one of the earliest and simplest methods of encryption technique. It's simply a type of substitution cipher, i.e., each letter of a given text is replaced by a letter with a fixed number of positions down the alphabet. For example with a **shift** of 1, A would be replaced by B, B would become C, and so on.

Caesar cipher

- Encryption:
  - Enc(x) = (x + k) mod N
- Decryption:
  - Dec(y) = (y − k) mod N

- X = message
- Y = encrypted message
- K = key
- Mod = Modulo operation
- N = is the number of alphabet

Modulo operation

- 7 mod 3 = 1
  - 7 / 3 = 2 Rest: 1
- 3 mod 7 = 3
  - 3 / 7 = 0 Rest = 3

Caesar

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

Encryption

- x = HELLOWORLD
- k = 8
- Enc(x) = (x + k) mod N

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

„x“	H	E	L	L	O	W	O	R	L	D
	7	4	11	11	14	22	14	17	11	3
„k“	8	8	8	8	8	8	8	8	8	8
	15	12	19	19	22	30 mod 26 = 4	22	25	19	11
„y“	P	M	T	T	W	E	W	Z	T	L

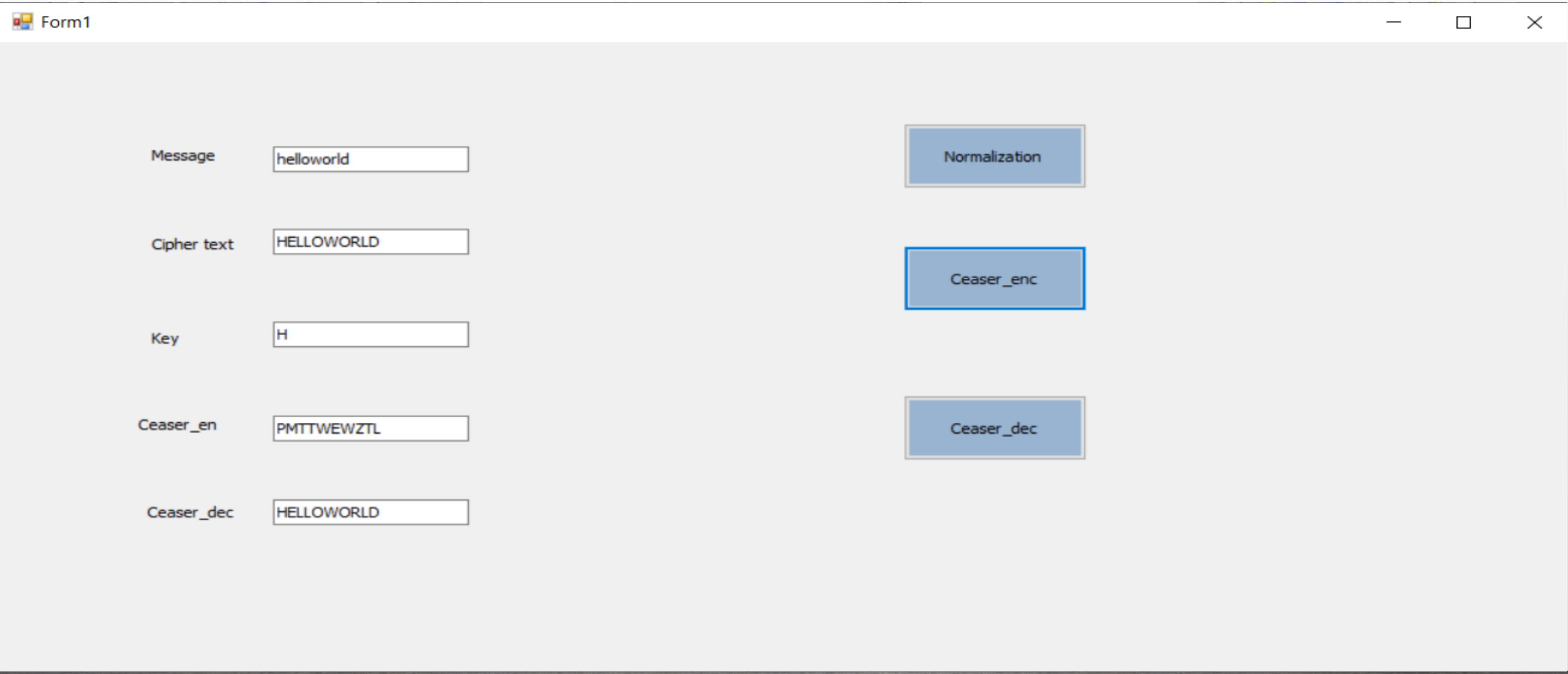
Decryption

- y = PMTTWEWZTL
- Dec(y) = (x - k) mod N
- Brute force

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

„y“	P	M	T	T	W	E	W	Z	T	L
K=8	H	E	L	L	O	W	O	R	L	D

Caesar


Form1
Message
helloworld
Cipher text
HELLOWORLD
Key
H
Ceaser_en
PMTTWEWZTL
Ceaser_dec
HELLOWORLD
Normalization
Ceaser_enc
Ceaser_dec