Plaintext: PADDLE

KEY: RED

Input:

P	A	D	D	L	W
R	E	D	R	E	D

The key is padded (repeated) to match the length of the plaintext

	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

→ Encryption

P & R → G, A & E → E, D & D → G, D & R → U, L & E → P, E & D → H

Cyphertext = GEGUPH

➔ **Decryption**

Input:

G	E	G	U	P	H
R	E	D	R	E	D

G & R → P, E & E → A, G & D → D, U & R → D, P & E → L, H & D → E

Plaintext: PADDLE

ALGEBRAIC REPRESENTATION

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

Plaintext: PADDLE

KEY: RED

➔ **Encryption**

$C_i = (M_i + K) \bmod 26$

C is the cypher text,

M is the plain text

K is the key

26 is the number of alphabets

M_1 = P = 15, K = R =17

$C_1 = (15 + 17) \bmod 26$

$C_1 = 32 \bmod 26$

$C_1 = 6 = G$

M_2 = A = 0, K = E = 4

$C_2 = (0 + 4) \bmod 26$

$C_2 = 4 \bmod 26$

$C_2 = 4 = E$

M_3 = D = 3, K = D = 3

$C_3 = (3 + 3) \bmod 26$

$C_3 = 6 \bmod 26$

$C_3 = 6 = G$

$M_4 = D = 3, K = R = 17$

$C_4 = (3 + 17) \bmod 26$

$C_4 = 20 \bmod 26$

$C_4 = 20 = U$

$M_5 = L = 14, K = E = 4$

$C_5 = (11 + 4) \bmod 26$

$C_5 = 15 \bmod 26$

$C_5 = 15 = P$

$M_6 = E = 4, K = D = 3$

$C_6 = (4 + 3) \bmod 26$

$C_6 = 7 \bmod 26$

$C_6 = 7 = H$

Cyphertext = GEGUPH

➔ **Decryption**

$M_i = (C_i - K + 26) \bmod 26$

$C_1 = G = 6, K = R = 17$

$M_1 = (6 - 17 + 26) \bmod 26$

$M_1 = 15 \bmod 26$

$M_1 = 15 = P$

$C_2 = E = 4, K = E = 4$

$M_2 = (4 - 4 + 26) \bmod 26$

$M_2 = 26 \bmod 26$

$M_2 = 0 = A$

C_3 = G = 6, K = D = 3

M_3 = (6 - 3 + 26) mod 26

M_3 = 29 mod 26

M_3 = 3 = D

C_4 = U = 20, K = R = 17

M_4 = (20 - 17 + 26) mod 26

M_4 = 29 mod 26

M_4 = 3 = D

C_5 = P = 6, K =ER = 17

M_5 = (15 - 4 + 26) mod 26

M_5 = 37 mod 26

M_5 = 11 = L

C_6 = H = 7, K = D = 3

M_6 = (7 - 3 + 26) mod 26

M_6 = 30 mod 26

M_6 = 4 = E

Plaintext: PADDLE