

CAESER CIPHER

- Here we assign numbers 0-25 to the alphabets A-Z. Then we add a fixed offset of 3 i.e. $(P+3) \bmod 26$.

e.g. Message = "HAPPY"

Step 1

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								

H	A	P	P	Y
+3	+3	+3	+3	+3
K	D	S	S	B

Encrypted message (cipher) = "KDSSB"

K	D	S	S	B
-3	-3	-3	-3	-3
H	A	P	P	Y

← original message -

• Here we assign numbers 0-25 to the alphabets A-Z. Then we add a fixed offset of 3 i.e. $(P_i + 3) \bmod 26$.

Page 1

A	0	B	1	C	2	D	3	E	4
F	5	G	6	H	7	I	8	J	9
K	10	L	M	N	O	P	Q	R	S
T	U	V	W	X	Y	Z	aa	ab	ac
ad	ae	af	ag	ah	ai	aj	ak	al	am
an	ao	ap	aq	ar	as	at	au	av	aw
ax	ay	az	ba	bb	bc	bd	be	bf	bg
bh	bi	bj	bk	bl	bm	bn	bo	bp	bq
br	bs	bt	bu	bv	bw	bx	by	bz	ca
cb	cc	cd	ce	cf	cg	ch	ci	cj	ck
cl	cm	cn	co	cp	cq	cr	cs	ct	cu
cv	cw	cx	cy	cz	da	db	dc	dd	de
df	dg	dh	di	dj	dk	dl	dm	dn	do
dp	dq	dr	ds	dt	du	dv	dw	dx	dy
dz	ea	eb	ec	ed	ee	ef	eg	eh	ei
ej	ek	el	em	en	eo	ep	eq	er	es
et	eu	ev	ew	ex	ey	ez	fa	fb	fc
fd	fe	ff	fg	fh	fi	fj	fk	fl	fm
fn	fo	fp	fq	fr	fs	ft	fu	fv	fw
fx	fy	fz	ga	gb	gc	gd	ge	gf	gg
gh	gi	gj	gk	gl	gm	gn	go	gp	gq
gr	gs	gt	gu	gv	gw	gx	gy	gz	ha
hb	hc	hd	he	hf	hg	hh	hi	hj	hk
hl	hm	hn	ho	hp	hq	hr	hs	ht	hu
hv	hw	hx	hy	hz	ia	ib	ic	id	ie
if	ig	ih	ii	ij	ik	il	im	in	io
ip	iq	ir	is	it	iu	iv	iw	ix	iy
iz	ja	jb	jc	jd	je	jf	jj	jk	jl
jm	jn	jo	jp	jq	jr	js	jt	ju	jv
jw	jx	ji	jj	jk	jl	jm	jn	jo	jp
jq	jr	js	jt	ju	jv	jw	jx	ji	jj
jk	jl	jm	jn	jo	jp	jq	jr	js	jt
ju	jv	jw	jx	ji	jj	jk	jl	jm	jn
jo	jp	jq	jr	js	jt	ju	jv	jw	jx
ji	jj	jk	jl	jm	jn	jo	jp	jq	jr
js	jt	ju	jv	jw	jx	ji	jj	jk	jl
jm	jn	jo	jp	jq	jr	js	jt	ju	jv
jw	jx	ji	jj	jk	jl	jm	jn	jo	jp
jq	jr	js	jt	ju	jv	jw	jx	ji	jj
jk	jl	jm	jn	jo	jp	jq	jr	js	jt
ju	jv	jw	jx	ji	jj	jk	jl	jm	jn
jo	jp	jq	jr	js	jt	ju	jv	jw	jx
ji	jj	jk	jl	jm	jn	jo	jp	jq	jr
js	jt	ju	jv	jw	jx	ji	jj	jk	jl
jm	jn	jo	jp	jq	jr	js	jt	ju	jv
jw	jx	ji	jj	jk	jl	jm	jn	jo	jp
jq	jr	js	jt	ju	jv	jw	jx	ji	jj
jk	jl	jm	jn	jo	jp	jq	jr	js	jt
ju	jv	jw	jx	ji	jj	jk	jl	jm	jn
jo	jp	jq	jr	js	jt	ju	jv	jw	jx
ji	jj	jk	jl	jm	jn	jo	jp	jq	jr
js	jt	ju	jv	jw	jx	ji	jj	jk	jl
jm	jn	jo	jp	jq	jr	js	jt	ju	jv
jw	jx	ji	jj	jk	jl	jm	jn	jo	jp
jq	jr	js	jt	ju	jv	jw	jx	ji	jj
jk	jl	jm	jn	jo	jp	jq	jr	js	jt
ju	jv	jw	jx	ji	jj	jk	jl	jm	jn
jo	jp	jq	jr	js	jt	ju	jv	jw	jx
ji	jj	jk	jl	jm	jn	jo	jp	jq	jr
js	jt	ju	jv	jw	jx	ji	jj	jk	jl
jm	jn	jo	jp	jq	jr	js	jt	ju	jv
jw	jx	ji	jj	jk	jl	jm	jn	jo	jp
jq	jr	js	jt	ju	jv	jw	jx	ji	jj
jk	jl	jm	jn	jo	jp	jq	jr	js	jt
ju	jv	jw	jx	ji	jj	jk	jl	jm	jn
jo	jp	jq	jr	js	jt	ju	jv	jw	jx
ji	jj	jk	jl	jm	jn	jo	jp	jq	jr
js	jt	ju	jv	jw	jx	ji	jj	jk	jl
jm	jn	jo	jp	jq	jr	js	jt	ju	jv
jw	jx	ji	jj	jk	jl	jm	jn	jo	jp
jq	jr	js	jt	ju	jv	jw	jx	ji	jj
jk	jl	jm	jn	jo	jp	jq	jr	js	jt
ju	jv	jw	jx	ji	jj	jk	jl	jm	jn
jo	jp	jq	jr	js	jt	ju	jv	jw	jx
ji	jj	jk	jl	jm	jn	jo	jp	jq	jr
js	jt	ju	jv	jw	jx	ji	jj	jk	jl
jm	jn	jo	jp	jq	jr	js	jt	ju	jv
jw	jx	ji	jj	jk	jl	jm	jn	jo	jp
jq	jr	js	jt	ju	jv	jw	jx	ji	jj
jk	jl	jm	jn	jo	jp	jq	jr	js	jt
ju	jv	jw	jx	ji	jj	jk	jl	jm	jn
jo	jp	jq	jr	js	jt	ju	jv	jw	jx
ji	jj	jk	jl	jm	jn	jo	jp	jq	jr
js	jt	ju	jv	jw	jx	ji	jj	jk	jl
jm	jn	jo	jp	jq	jr	js	jt	ju	jv
jw	jx	ji	jj	jk	jl	jm	jn	jo	jp
jq	jr	js	jt	ju	jv	jw	jx	ji	jj
jk	jl	jm	jn	jo	jp	jq	jr	js	jt
ju	jv	jw	jx	ji	jj	jk	jl	jm	jn
jo	jp	jq	jr	js	jt	ju	jv	jw	jx
ji	jj	jk	jl	jm	jn	jo	jp	jq	jr
js	jt	ju	jv	jw	jx	ji	jj	jk	jl
jm	jn	jo	jp	jq	jr	js	jt	ju	jv
jw	jx	ji	jj	jk	jl	jm	jn	jo	jp
jq	jr	js	jt	ju	jv	jw	jx	ji	jj
jk	jl	jm	jn	jo	jp	jq	jr	js	jt
ju	jv	jw	jx	ji	jj	jk	jl	jm	jn
jo	jp	jq	jr	js	jt	ju	jv	jw	jx
ji	jj	jk	jl	jm	jn	jo	jp	jq	jr
js	jt	ju	jv	jw	jx	ji	jj	jk	jl
jm	jn	jo	jp	jq	jr	js	jt	ju	jv
jw	jx	ji	jj	jk	jl	jm	jn	jo	jp
jq	jr	js	jt	ju	jv	jw	jx	ji	jj
jk	jl	jm	jn	jo	jp	jq	jr	js	jt
ju	jv	jw	jx	ji	jj	jk	jl	jm	jn
jo	jp	jq	jr	js	jt	ju	jv	jw	jx
ji	jj	jk	jl	jm	jn	jo	jp	jq	jr
js	jt	ju	jv	jw	jx	ji	jj	jk	jl
jm	jn	jo	jp	jq	jr	js	jt	ju	jv
jw	jx	ji	jj	jk	jl	jm	jn	jo	jp
jq	jr	js	jt	ju	jv	jw	jx	ji	jj
jk	jl	jm	jn	jo	jp	jq	jr	js	jt
ju	jv	jw	jx	ji	jj	jk	jl	jm	jn
jo	jp	jq	jr	js	jt	ju	jv	jw	jx
ji	jj	jk	jl	jm	jn	jo	jp	jq	jr
js	jt	ju	jv	jw	jx	ji	jj	jk	jl
jm	jn	jo	jp	jq	jr	js	jt	ju	jv
jw	jx	ji	jj	jk	jl	jm	jn	jo	jp
jq	jr	js	jt	ju	jv	jw	jx	ji	jj
jk	jl	jm	jn	jo	jp	jq	jr	js	jt
ju	jv	jw	jx	ji	jj	jk	jl	jm	jn
jo	jp	jq	jr	js	jt	ju	jv	jw	jx
ji	jj	jk	jl	jm	jn	jo	jp	jq	jr
js	jt	ju	jv	jw	jx	ji	jj	jk	jl
jm	jn	jo	jp	jq	jr	js	jt	ju	jv
jw	jx	ji	jj	jk	jl	jm	jn	jo	jp
jq	jr	js	jt	ju	jv	jw	jx	ji	jj
jk	jl	jm	jn	jo	jp	jq	jr	js	jt
ju	jv	jw	jx	ji	jj	jk	jl	jm	jn
jo	jp	jq	jr	js	jt	ju	jv	jw	jx
ji	jj	jk	jl	jm	jn	jo	jp	jq	jr
js	jt	ju	jv	jw	jx	ji	jj	jk	jl
jm	jn	jo	jp	jq	jr	js	jt	ju	jv
jw	jx	ji	jj	jk	jl	jm	jn	jo	jp
jq	jr	js	jt	ju	jv	jw	jx	ji	jj
jk	jl	jm	jn	jo	jp	jq	jr	js	jt
ju	jv	jw	jx	ji	jj	jk	jl	jm	jn
jo	jp	jq	jr	js	jt	ju	jv	jw	jx
ji	jj	jk	jl	jm	jn	jo	jp	jq	jr
js	jt	ju	jv	jw	jx	ji	jj	jk	jl
jm	jn	jo	jp	jq	jr	js	jt	ju	jv
jw	jx	ji	jj	jk	jl	jm	jn	jo	jp
jq	jr	js	jt	ju	jv	jw	jx	ji	jj
jk	jl	jm	jn	jo	jp	jq	jr	js	jt
ju	jv	jw	jx	ji	jj	jk	jl	jm	jn
jo	jp	jq	jr	js	jt	ju	jv	jw	jx
ji	jj	jk	jl	jm	jn	jo	jp	jq	jr
js	jt	ju	jv	jw	jx	ji	jj	jk	jl
jm	jn	jo	jp	jq	jr	js	jt	ju	jv
jw	jx	ji	jj	jk	jl	jm	jn	jo	jp
jq	jr	js	jt	ju	jv	jw	jx	ji	jj
jk	jl	jm	jn	jo	jp	jq	jr	js	jt
ju	jv	jw	jx	ji	jj	jk	jl	jm	jn
jo	jp	jq	jr	js	jt	ju	jv	jw	jx
ji	jj	jk	jl	jm	jn	jo	jp	jq	jr
js	jt	ju	jv	jw	jx	ji	jj	jk	jl
jm	jn	jo	jp	jq	jr	js	jt	ju	jv
jw	jx	ji	jj	jk	jl	jm	jn	jo	jp
jq	jr	js	jt	ju	jv	jw	jx	ji	jj
jk	jl	jm	jn	jo	jp	jq	jr	js	jt
ju	jv	jw	jx	ji	jj	jk	jl	jm	jn
jo	jp	jq	jr	js	jt	ju	jv	jw	jx
ji	jj	jk	jl	jm	jn	jo	jp	jq	jr
js	jt	ju	jv	jw	jx	ji	jj	jk	jl
jm	jn	jo	jp	jq	jr	js	jt	ju	jv
jw	jx	ji	jj	jk	jl	jm	jn	jo	jp
jq	jr	js	jt	ju	jv	jw	jx	ji	jj
jk	jl	jm	jn	jo	jp	jq	jr	js	jt
ju	jv	jw	jx	ji	jj	jk	jl	jm	jn
jo	jp	jq	jr	js	jt	ju	jv	jw	jx
ji	jj	jk	jl	jm	jn	jo	jp	jq	jr
js	jt	ju	jv	jw	jx	ji	jj	jk	jl
jm	jn	jo	jp	jq	jr	js	jt	ju	jv
jw	jx	ji	jj	jk	jl	jm	jn	jo	jp
jq	jr	js	jt	ju	jv	jw	jx	ji	jj
jk	jl	jm	jn	jo	jp	jq	jr	js	jt
ju	jv	jw	jx	ji	jj	jk	jl	jm	jn
jo	jp	jq	jr	js	jt	ju	jv	jw	jx
ji	jj	jk	jl	jm	jn	jo	jp	jq	jr
js	jt	ju	jv	jw	jx	ji	jj	jk	jl
jm	jn	jo	jp	jq	jr	js	jt	ju	jv
jw	jx	ji	jj	jk	jl	jm	jn	jo	jp
jq	jr	js	jt	ju	jv	jw	jx	ji	jj
jk	jl	jm	jn	jo	jp	jq	jr	js	jt
ju	jv	jw	jx	ji	jj	jk	jl	jm	jn
jo	jp	jq	jr	js	jt	ju	jv	jw	jx
ji	jj	jk	jl	jm	jn	jo	jp	jq	jr
js	jt	ju	jv	jw	jx	ji	jj	jk	jl
jm	jn	jo	jp	jq	jr	js	jt	ju	jv
jw	jx	ji	jj	jk	jl	jm	jn	jo	jp
jq	jr	js	jt	ju	jv	jw	jx	ji	jj
jk	jl	jm	jn	jo	jp	jq	jr	js	jt
ju	jv	jw	jx	ji	jj	jk	jl	jm	jn
jo	jp	jq	jr	js	jt	ju	jv		

H	A	P	P	Y
+2	+3	+2	+3	+3
K	D	S	S	B

Encrypted message
(cipher)
= "K D S S B"

K	D	S	S	B
-3	-3	-3	-3	-3
H	A	P	P	Y

← original message -

VIGENERE CIPHER

VIGENERE CIPHER

- Mostly used for text message encoding and decoding.
- We use a text "key" to encode a text "message"
- For encoding we use the formula
$$C_i = (P_i + K_i) \bmod 26,$$
where
 - C_i = code corresponding to P_i (plain text)
 - P_i = i th letter in the message.
 - K_i = key element
- We assign numbers 0-25 to the letters A-Z
- For decoding (reverse process) we use
$$P_i = (C_i - K_i) \bmod 26.$$
 - * if $(C_i - K_i) < 0$ we add 26.

Show how you can encode and decode the message "MILLION" using the Vigenere cipher. The encryption key is "SKY".

2. We assign values to letters A-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	Z						

02

M	I	L	L	I	O	N
S	K	Y	S	K	Y	S

3

$P_i + K_i$	C_i	$C_i \% 26$	
$M + S$	$12 + 18$	04	E
$I + K$	$8 + 10$	18	S
$L + Y$	$11 + 24$	09	J
$L + S$	$11 + 18$	03	D
$I + K$	$8 + 10$	18	S
$O + Y$	$14 + 24$	12	M
$N + S$	$13 + 18$	05	F

The cipher or encrypted message is "ESTDSMF"

For decryption:-

Step 1: Use the same table in encryption

Step 2:

E	S	J	D	S	M	F
S	K	Y	S	K	Y	S

Step 3:

$C_i - K_i$	P_i	$P_i \% 26$	P_m
E - S	4 - 18	12	M
S - K	18 - 10	08	I
J - Y	9 - 24	11	L
D - S	3 - 18	11	L
S - K	18 - 10	08	I
M - S Y	12 - 24	14	O
F - S	5 - 18	13	N

If the difference \uparrow \uparrow
is negative, add 26.

AFFINE CIPHER

Affine cipher uses the formula

$$C = \text{ax} + (ax+b) \bmod m$$

Here $a=9$, $b=2$, $m=26$.

$$C = (9x+2) \bmod 26$$

$C = (9x+2) \% 26$

m	U	K	R	A	I	N	E	
x	20	10	17	0	8	13	4	
	A	m	Z	C	W	P	M	

ciphertext = "AmZCWPM"

5) We have to find inverse of a (call it y)

Such that $a \cdot y \equiv 1 \bmod m$.

$$\text{ie } (a \cdot y) \bmod m = 1$$

$$\text{ie } (9 \cdot y) \bmod 26 = 1$$

y	a.y	(a.y) % 26
1	9	9
2	18	18
3	27	1

$$\therefore y = 3$$

For decryption we use the formula

$$m = y(c - b) \bmod 26 = 3(c - 2) \% 26$$

$c \Rightarrow$	A	m	Z	C	W	P	m
$x \Rightarrow$	0	12	25	2	22	15	12
$m \Rightarrow$ $(x-2) \% 26$	U	K	R	A	I	N	E