ADFGVX cipher :

PASSWORD : CROP (common knowledge)

COPR

	A	D	F	G	V	X
A	1	2	A	B	0	3
D	C	D	4	5	E	F
F	6	7	G	H	I	8
G	K	L	M	9	N	O
V	P	Q	R	S	T	U
X	V	W	X	X	Z	J

(common knowledge)

Some message was sent. ~~RE~~ Received message is

V A V D A A G F ↓ F V X F V F F V F G V A V A F ~~V G D V A A~~ D

VGDVAAD

30 = 7×4+2

C	O	P	R
V	V	F	V
A	G	V	F
V	D	X	G
D	V	F	V
A	A	V	A
A	A	F	V
G	D	F	A
F			F

C	R	O	P	
V	V	V	F	✓
A	F	G	V	✓
V	G	D	X	✓
D	V	V	F	✓
A	A	A	V	✓
A	V	A	F	✓
G	A	D	F	✓
F	F			

VV VF AF GV DG DX DV VF AA AV

✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓

AV AF GA AF FF → D

✓ ✓ ✓ ✓ ✓

TRANSFER 100 AK47

Permutation cipher.

1	2	3	4	5	6	7	8	9	10	11	12	13	14
A	B	C	D	E	F	G	H	I	J	K	L	M	N

15	16	17	18	19	20	21	22	23	24	25	26
O	P	Q	R	S	T	U	V	W	X	Y	Z

$\sigma \in S_{26}$

$$\mathcal{E}(x_{i_1} x_{i_2} \cdots x_{i_k}) = x_{\sigma(i_1)} x_{\sigma(i_2)} \cdots x_{\sigma(i_k)}$$

$$\& \quad \mathcal{D}(y_{i_1} y_{i_2} \cdots y_{i_k}) = y_{\sigma^{-1}(i_1)} y_{\sigma^{-1}(i_2)} \cdots y_{\sigma^{-1}(i_k)}$$

Aside

$X = \{x_1, x_2, \dots, x_n\}$ so that $|X| = n$.

$\sigma : X \longrightarrow X$ a bijection. called a permutation

E.g. $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} = (1)(2\ 4\ 3)$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 6 & 1 & 2 & 5 & 8 & 7 \end{pmatrix}$$

$$= \underbrace{(1\ 3\ 6\ 5\ 2\ 4)}\ \underbrace{(7\ 8)}$$

$\boxed{\begin{array}{l} (\tau\sigma)^{-1} = \sigma^{-1}\tau^{-1} \\ \text{If } \tau \ \& \ \sigma \text{ are distinct cycles then } \tau\sigma = \sigma\tau. \end{array}}$

Any permutation is a product of distinct cycles

How to multiply: $(1\ 2\ 3)(2\ 4\ 5)$

$$= (1\ 2\ 4\ 5\ 3)$$

Inverse of $(x_1\ x_2 \cdots x_k)$ is $(x_1\ x_2 \cdots x_k)^{-1} = (x_k\ x_{k-1} \cdots x_1)$

e.g. $(1\ 2)^{-1} = (2\ 1) = (1\ 2)$. $(1\ 2\ 3)^{-1} = (3\ 2\ 1) = (1\ 3\ 2)$

$\sigma = (1\ \ 15\ \ 21)\ (13\ \ 3\ \ 5)$ ✓

$\sigma^{-1} = (1\ \ \underbrace{21\ \ 15})\ (3\ \ 13\ \ 5)$

Recived message (i.e. cipher text)

YUA COYEUCM

$25-21-1-3-15-25-5-21-3-13 \xrightarrow{\sigma^{-1}} 25-15-21-13-1-25-3-15-13-5$

plain text YOU MAY COME

To construct σ (the permutation) use a password.

Eg. password CROSS WORD → CDORSW

A	B	C	D	E	F	G	H	I	J	K	L	M	N
C	D	O	R	S	W	A	B	E	F	G	H	I	J

O	P	Q	R	S	T	U	V	W	X	Y	Z
K	L	M	N	P	Q	T	U	V	X	Y	Z

$\sigma = (A\ C\ O\ K\ G)\ (B\ D\ R\ N\ J\ F\ W\ V\ U\ T\ Q\ M\ I\ E\ S\ P\ L\ H)$

$\sigma^{-1} = (A\ G\ K\ O\ C)\ (B\ H\ L\ P\ S\ E\ I\ M\ Q\ T\ U\ V\ W\ F\ J\ N\ R\ D)$