Transposition techniques

- **Transposition techniques** systematically transpose the position of plaintext elements.

- **Rail Fence Technique**

- In this technique text is written down as a sequence of diagonals and then read of as sequence of rows.

Transposition techniques (Conti…)

- Plain text: meet at five pm behind p lab.
- Written as rail fence of depth 2:

m		e		a		f		v		p		b		h		n		p		a	
	e		t		t		i		e		m		e		i		d		l		b

- Encrypted as: mea fvp bhn pae tti eme idl b

- With rail fence of depth 3:

- Encrypted as: mtf ebi pbe aip enl xet vmh dax

M			T			F			E			B			I			P			B		
	E			A			I			P			E			N			L			X	
		E			T			V			M			H			D			A			X

Transposition techniques (Conti…)

- A more complex scheme is to write a message in a rectangle (square matrix), row-by-row and read it off, column.

- Pain text: meet at five pm behind p lab.

m	e	e	t	a
t	f	i	v	e
p	m	b	e	h
i	n	d	p	l
a	b	x	x	x

- Encrypted text: mtpiaefmnbeibdxtvepxaehlx

Transposition techniques (Conti…)

- Alternatively, a key can also be defined to permute the order of the column, e.g. encryption key (41523) defines write in a row-by-row, read it off: 4th column first, 1st column second, 5th column third, followed by 2nd and 3rd column, and prepare encrypted text.