

INFORMATION THEORY

Playfair Cipher

WEEK 6

ENCRYPTION TECHNIQUE

-The Algorithm consists of 2 steps:

1- Generate the key Square(5×5)

- The key square is a 5×5 grid of alphabets that acts as the key for encrypting the plaintext. Each of the 25 alphabets must be unique and one letter of the alphabet (**usually J**) is omitted from the table (as the table can hold only 25 alphabets). If the plaintext contains J, then it is replaced by I.
- The initial alphabets in the key square are the unique alphabets of the key in the order in which they appear followed by the remaining letters of the alphabet in order.

ENCRYPTION TECHNIQUE

- The Encryption key is “playfair”

p	l	a	y	f
i	r	b	c	d
e	g	h	k	m
n	o	q	s	t
u	v	w	x	z

ENCRYPTION TECHNIQUE

- Step 2:

1. The plaintext is split into pairs of two letters (digraphs). If there is an odd number of letters, a Z is added to the last letter.

PlainText: "instruments"

After Split: 'in'

'st'

'ru'

'me'

'nt'

'sZ'

ENCRYPTION TECHNIQUE

❑ Rules for Encryption:

- ✓ **If both the letters are in the same column:** Take the letter below each one (going back to the top if at the bottom).
- ✓ **If both the letters are in the same row:** Take the letter to the right of each one (going back to the leftmost if at the rightmost position).
- ✓ **If neither of the above rules is true:** Form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.

ENCRYPTION TECHNIQUE

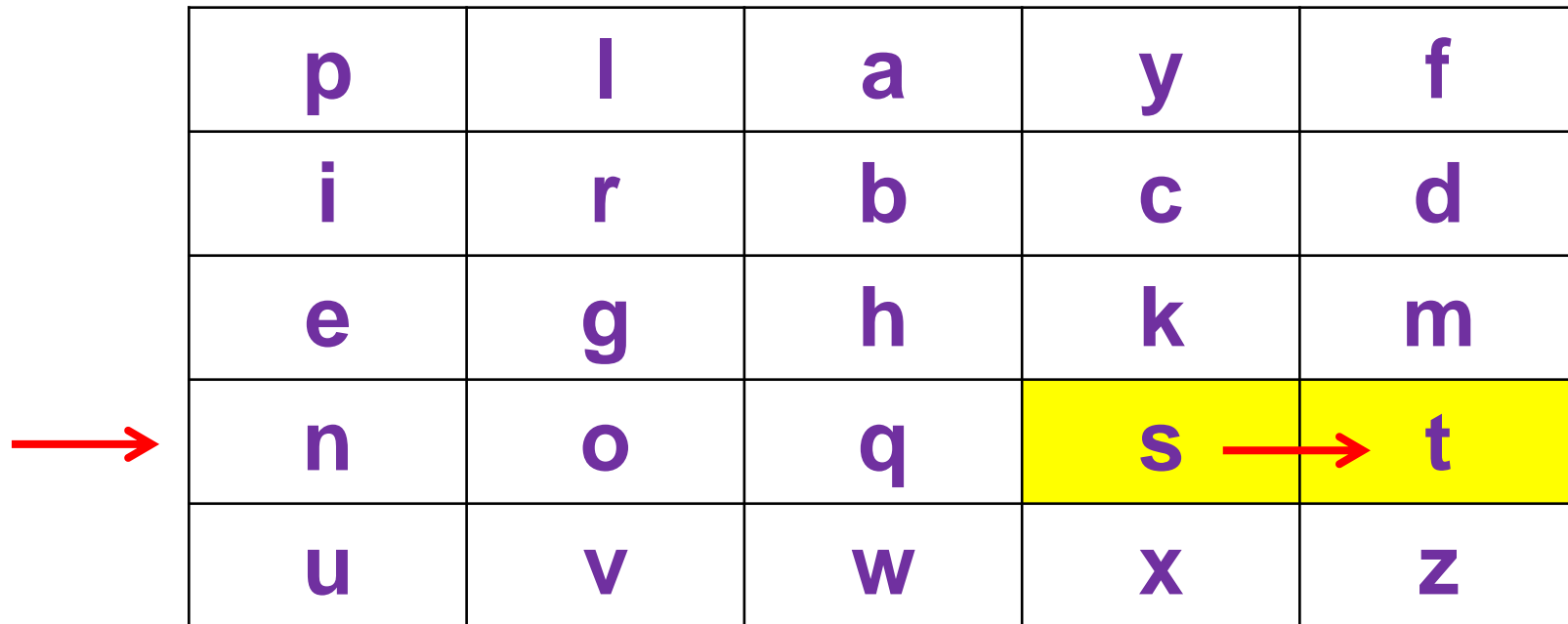
p	l	a	y	f
i	r	b	c	d
e	g	h	k	m
n	o	q	s	t
u	v	w	x	z

ENCRYPTION TECHNIQUE

	p	l	a	y	f
	i	r	b	c	d
→	e	g	h	k	m
	n	o	q	s	t
→	u	v	w	x	z

- 'in' -> 'eu'

ENCRYPTION TECHNIQUE



p	l	a	y	f
i	r	b	c	d
e	g	h	k	m
n	o	q	s	t
u	v	w	x	z

- 'st' -> 'tn'

ENCRYPTION TECHNIQUE

p	l	a	y	f
i	r	b	c	d
e	g	h	k	m
n	o	q	s	t
u	v	w	x	z

- 'ru' -> 'iv'

ENCRYPTION TECHNIQUE

p	l	a	y	f
i	r	b	c	d
e	g	h	k	m
n	o	q	s	t
u	v	w	x	z

- 'me' -> 'eg'

ENCRYPTION TECHNIQUE

p	l	a	y	f
i	r	b	c	d
e	g	h	k	m
n	o	q	s	t
u	v	w	x	z

- 'nt' -> 'on'

ENCRYPTION TECHNIQUE

p	l	a	y	f
i	r	b	c	d
e	g	h	k	m
n	o	q	s	t
u	v	w	x	z

- 'sz' -> 'tx'

“instruments” = “eutnivegontx”

DECRYPTION TECHNIQUE

- For both **encryption** and **decryption**, the **same key** is to be used.
- Decrypting the Playfair cipher is as simple as doing the same process **in reverse**.

❑ Rules for Decryption:

- ✓ **If both the letters are in the same column:** Take the letter above each one.
- ✓ **If both the letters are in the same row:** Take the letter to the left of each one
- ✓ **If neither of the above rules is true:** Form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.

DECRYPTION TECHNIQUE

- The Decryption key is “**playfair**”.
- Ciphertext: “**eutnivegontx**”
- Split Ciphertext: “**eu**” - “**tn**” - “**iv**” - “**eg**” - “**on**” - “**tx**”

p	l	a	y	f
i	r	b	c	d
e	g	h	k	m
n	o	q	s	t
u	v	w	x	z

DECRYPTION TECHNIQUE

p	l	a	y	f
i	r	b	c	d
e	g	h	k	m
n	o	q	s	t
u	v	w	x	z

DECRYPTION TECHNIQUE

p	l	a	y	f
i	r	b	c	d
e	g	h	k	m
n	o	q	s	t
u	v	w	x	z

DECRYPTION TECHNIQUE

p	l	a	y	f
i	r	b	c	d
e	g	h	k	m
n	o	q	s	t
u	v	w	x	z

DECRYPTION TECHNIQUE

p	l	a	y	f
i	r	b	c	d
e	g	h	k	m
n	o	q	s	t
u	v	w	x	z

DECRYPTION TECHNIQUE

p	l	a	y	f
i	r	b	c	d
e	g	h	k	m
n	o	q	s	t
u	v	w	x	z

DECRYPTION TECHNIQUE

p	l	a	y	f
i	r	b	c	d
e	g	h	k	m
n	o	q	s	t
u	v	w	x	z

- Ciphertext: “eutnivegontx” -> Plaintext: “instrumentsz”