

④ Playfair cipher :-

→ ① Aka Playfair Square or Wheatstone - playfair cipher.

- ② Manual symmetric encryption technique.
- ③ First literal digram substitution cipher
- ④ Invented in 1854 by Charles Wheatstone
- ⑤ Bore the name of Lord playfair for promoting its use.

→ ① Multiple letter encryption cipher

② Digrams

③ 5x5 matrix constructed using a keyword

→ Rules for encryption Using Playfair cipher.

- ① Digrams
- ② Repeating letters - filler letter
- ③ same column | ↓ | wrap around
- ④ same row | → | wrap around
- ⑤ Rectangle | ↗ ↘ | swap

Plaintext → attack
Digrams → at ta ck

Plaintext → neso academy
Digrams → ne so ac ad em yx

Plaintext → balloon
ba ll oo n ⇒ filler letter x
ba lx lo on.

Ex., cipher is keyed by a word COMPUTER

| | | | | |
|---|---|---|---|-----|
| C | O | M | P | U |
| T | E | R | A | B |
| D | F | G | H | I/J |
| K | L | N | Q | S |
| V | W | X | Y | Z |

5x5

Plaintext :- CNSHCI
Digram :-

| | | |
|----|----|----|
| CN | SH | CI |
| KM | QI | DU |

— x —

key :- MONARCHY
 ② Ex., Plaintext :- attack
 digram :-

| | | |
|----|----|----|
| at | ta | ck |
| RS | SR | DE |

| | | | | |
|---|---|---|-----|---|
| M | O | N | A | R |
| C | H | Y | B | D |
| E | F | G | I/J | K |
| L | P | Q | S | T |
| U | V | W | X | Z |

5x5

③ cipher is keyed by a word
 key :- COMPUTER

| | | | | |
|---|---|---|---|-----|
| C | O | M | P | U |
| T | E | R | A | B |
| D | F | G | H | I/J |
| K | L | N | Q | S |
| V | W | X | Y | Z |

please transfer one million dollars
 to my account six six two

Note →

- 1) OF → EI
- 2) LW → WD
- 3) RA → AB
- 4) ZV → VW
- 5) UT → CB

| | | | | | | | | | | |
|---------------|----|----|----|----|---------------|----|----|---------------|----|---------------|
| PL | EA | SE | TR | AN | SF | ER | ON | EM | IL | LI |
| 00 | RB | LB | EA | RQ | ZI | RA | ML | RO | FS | SF |
| ON | DO | IX | LA | YS | TO | MY | AC | CO | UN | |
| ML | FC | NW | GE | BN | EC | PX | TP | OM | MS | |
| TS | IC | SI | XT | WO | | | | | | |
| BK | GZ | ZJ | VR | OE | | | | | | |

— x —

④ Ex., Heya → He ya

abhi

| | | | | |
|---|---|---|-----|---|
| A | B | H | I/J | C |
| ① | E | F | G | K |
| L | M | N | O | P |
| Q | R | S | T | U |
| V | W | X | Y | Z |

Hello → He lx lo

Helloe → He lx lo ez

Hexxoe → He xz xo ez

| | | |
|----|---|----|
| BM | → | ER |
| RW | → | WB |
| FG | → | GK |
| UQ | → | QR |
| KL | → | DP |
| SK | → | FU |

— x —

④ Playfair cipher :-

→ ① Aka Playfair Square or Wheatstone - playfair cipher.

- ② Manual symmetric encryption technique.
- ③ First literal digram substitution cipher
- ④ Invented in 1854 by Charles Wheatstone
- ⑤ Bore the name of Lord playfair for promoting its use.

→ ① Multiple letter encryption cipher

② Digrams

③ 5x5 matrix constructed using a keyword

→ Rules for encryption Using Playfair cipher.

- ① Digrams
- ② Repeating letters — filler letter
- ③ Same column | ↓ | wrap around
- ④ same row | → | wrap around
- ⑤ Rectangle | ↗ ↘ | swap.