**PRACTICAL-2**

**AIM:**

Provide the extended version of Play-Fair cipher after launching Brute-Force attack in Practical-1. [Hint. Use extended matrix size, which incorporates variety of symbols like alphabets, number, special symbol]

**Theory:**

We have play-Fair(5\*5) technique already then what is the need of it’s extended one. Here we know that in 5\*5 play-fair matrix we use alphabets(A-Z) for encryption, but in case of extended play-fair matrix there will be 6\*6 matrix so here with the alphabets we have to also use (0-9) numbers to make the matrix complete. And for 7\*7 we can use some other symbols like %,&,?.

Now because of the use of numbers along with alphabets Extended play-fair will provide stronger encryption than simple play-fair, and it will be difficult for cracking the real text.

* **EXAMPLE OF 6\*6 PLAY-FAIR:**
* **KEY:** CHARUSAT
* **TEXT:**HELLO WORLD

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

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **PT:** | HE | LX | LO | WO | RL | DX |
| **CT:** | RB | NV | IV | PX | EV | GQ |

* **EXAMPLE OF 7\*7 PLAY-FAIR:**
* **KEY:**CHARUSAT
* **TEXT:**WELCOME MAN

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| C | H | A | R | U | S | T |
| B | D | E | F | G | I | J |
| K | L | M | N | O | P | Q |
| V | W | X | Y | Z | 0 | 1 |
| 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 9 | % | ^ | & | \* | ( | ) |
| ! | @ | # | $ | ? | { | } |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **PT:** | WE | LC | OM | EM | AN |
| **CT:** | XD | KH | PN | MX | RM |

**CONCLUSION:**

In this practical we have learnt about extended play-fair .